

CA2ΦN
AJ 810
-77P73

Public Government for Private People



**The Report of the Commission
on Freedom of Information
and Individual Privacy/1980**

**VOLUME 3
Protection of Privacy**



Digitized by the Internet Archive
in 2022 with funding from
University of Toronto

<https://archive.org/details/31761114687833>

Public Government for Private People



The Report of the Commission on Freedom of Information and Individual Privacy/1980

CA24N
AJ 8/0
-77P73

VOLUME 3
Protection of Privacy

Printed by J.C. Thatcher, Queen's Printer of Ontario

ISBN: The Report (3 volumes):0-7743-5432-1

ISBN: Volume 3:0-7743-5435-6

Available from the
Publications Centre
Ministry of Government Services
Queen's Park
Toronto, Ontario

or

Ontario Government Book Store
800 Bay Street
Toronto, Ontario



The Commission on Freedom of Information and Individual Privacy

D. Carlton Williams, Ph.D., LL.D., Chairman
G.H.U. Bayly, M.Sc.F., Commissioner
Dorothy J. Burgoyne, B.A., Commissioner
W.R. Poole, Q.C., Counsel and General Manager
J.D. McCamus, LL.M., Director of Research
Hon. J.C. McRuer, O.C., LL.D., D.C.L., Consultant
Doris E. Wagg, B.L.S., Registrar

Research Staff

Brenda R. Billingsley, M.A.
Timothy G.C. Brown, LL.B.
John Eichmanis, Ph.D.
Lawrence M. Fox, LL.B.
Heather Mitchell, LL.B.
S. Rebecca Shamai, LL.B.
Susan Soloway, M.A., LL.B.

Secretarial Staff

Rosemarie Aldridge
Inez Aziz
Natalie Gold
Victoria Van Asperen

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is to be communicated to others."

- Alan F. Westin, Privacy and Freedom

"In secrecy, law forbids the disclosure of information. In privacy, disclosure is at the discretion of the possessor..."

- Edward A. Shils

CHAPTER 25	A DEFINITION OF THE PRIVACY ISSUE	495
	A. Introduction	495
	B. Defining Privacy	498
	C. The Informational Privacy Issue	502
	D. Political Dimensions of the Issue	504
	E. Principles of Fair Information Practices	506
	F. Public Opinion	507
	G. Areas of Concern	510
	Public Knowledge of Personal Data	
	Banks	510
	Collection of Personal Information	510
	Maintenance of Data Integrity and	
	Security	510
	Transfer and Dissemination of	
	Personal Information	511
	Subject Access to Personal Records	511
	Computerization of Personal Records	511
CHAPTER 26	COMPUTERS AND PRIVACY	517
	A. The Computer's Effect on Privacy	517
	B. The Development of Computer Systems	519
	C. Security of Computerized Records	521
	D. Technological Change and Privacy	522
	E. Automation of Personal Records in	
	the Ontario Government	523
	F. Summary	525
CHAPTER 27	PERSONAL INFORMATION HANDLING PRACTICES OF	
	THE ONTARIO GOVERNMENT	531
	A. The Extent and Nature of Personal	
	Record Keeping	531
	Sources of Information About Government-	
	Held Records	531
	"What Do They Have On Me?"	533
	B. Previous Studies in Ontario	536
	Ontario Law Reform Commission	536
	Interministerial Committee on Privacy	538
	Privacy Project Task Group	539

C. Research Report Case Studies	542
Education	544
Government Personnel	547
Social Services	550
Law Enforcement	553
Corrections, Probation and Parole	560
Personal Property Security Registration System	562
Licensed Driver and Vehicle Ownership Records	564
Conclusions	567

CHAPTER 28 PERSONAL IDENTIFIERS: THE DEVELOPMENT
OF A SINGLE IDENTIFYING NUMBER 583

A. The Change from "Standard Identifiers" to Unique Personal Identifiers	583
B. Single Identifying Numbers	584
C. Personal Identifiers in the Ontario Government	586
D. The Growing Use of the Social Insurance Number	587

CHAPTER 29 DATA PROTECTION LAWS OF OTHER JURISDICTIONS 595

A. Introduction	595
B. Sweden	595
C. Other European Legislation	599
D. England: The Data Protection Committee	603
E. The United States: Federal Legislation	608
F. U.S. State Legislation	622
G. Canada: The Canadian Human Rights Act, Part IV	627
H. Canada: Provincial Privacy Legislation	636
I. New South Wales: The Privacy Committee	637

CHAPTER 30 THE LEGAL FRAMEWORK OF PRIVACY PROTECTION
IN ONTARIO 653

A. Introduction	653
B. The Common Law	653
C. Statutory Secrecy Provisions	656

CHAPTER 30 (Cont'd)

D. The Consumer Reporting Act and The Education Act	657
E. The Ontario Human Rights Code	662

CHAPTER 31 THE NEED FOR REFORM 667

CHAPTER 32 THE PROPOSED LEGISLATION: A GENERAL VIEW 675

A. Statutory Implementation of Fair Information Practices	675
B. Coverage of the Legislative Scheme	676
C. Administration and Enforcement	678
D. Recommendations	679

CHAPTER 33 THE STATUTORY IMPLEMENTATION OF FAIR
INFORMATION PRACTICES 681

A. A Public Record of Government Personal Data Banks	682
B. Collection of Personal Information	684
C. Standards for Maintaining the Integrity and Security of Data	690
D. Controlling Transfers of Data	693
E. Subject Access and Correction Rights	704
F. Research and Statistical Data	723
G. The Duty to Record Disclosures	727
H. Recommendations	732

CHAPTER 34 ADMINISTRATION AND ENFORCEMENT 747

A. The Role of the Ministries and Other Governmental Institutions	749
B. The "Responsible Keeper"	749
C. The Data Protection Authority	750
D. Dispute Resolution: Access and Correction Rights	754
E. The Interim and Transitional Phase: An Alternative Proposal	755
F. Recommendations	756

CHAPTER 35	CIVIL AND CRIMINAL LIABILITY	761
	A. Civil Liability: The Remedy of Monetary Damages	761
	B. The Establishment of Provincial or "Quasi-Criminal" Offences	764
	C. Recommendations	768
CHAPTER 36	REGULATING USE OF THE SOCIAL INSURANCE NUMBER	771
	Recommendations	776
CHAPTER 37	MAILING LISTS	779
	Recommendations	783
CHAPTER 38	TRANSBORDER DATA FLOWS	785
	Recommendations	787
CHAPTER 39	FREEDOM OF INFORMATION AND INDIVIDUAL PRIVACY	789
	A. The Personal Privacy Exemption to the FOI Scheme	790
	B. The Mandatory Nature of the FOI Privacy Exemption	791
	C. Integration of the Access Rights and Exemptions of the Two Schemes	792
	D. Integration of Procedural Mechanisms, Administrative Arrangements and Appeal Mechanisms	796
APPENDIX:	STATUTORY MATERIAL	799
	The Canadian Human Rights Act, Part IV	801
	The U.S. Privacy Act of 1974	807

A Definition of The Privacy Issue

A. INTRODUCTION

Although the "privacy problem" and the "right to privacy" are relatively recent arrivals on the agenda of public discussion in the Western industrialized democracies, the concept of personal privacy is of more ancient lineage. Indeed, there is considerable support for the view that the need of human beings for personal privacy is a universal, a common element in the human experience. It was evidenced in the social conditions of ancient Greece[1]. It is manifested in the customs and communal life of primitive tribes[2]. It is, in short, a fundamental and enduring human value. Some writers have suggested that privacy mechanisms are observable in the behaviour patterns of the animal world, and that perhaps a biological root is to be found at the bottom of this rather substantial behavioural tree[3]. Perceptions of the nature of and the need for privacy will vary among societal or cultural groups, and will change from one historical period to the next[4]. Within the same society, these perceptions will vary with individuals and evolve with changing social conditions. Nonetheless, the preservation of some measure of privacy or private life appears to be an essential feature of human existence.

It is striking, then, that widespread concern that the value of privacy in human life is being diminished and that corrective legislative measures are needed is a modern, and indeed, relatively recent, phenomenon. Is it true that the privacy values are more threatened in our time than they were in any other? We believe so; and it is not difficult to discern the reasons for the current level of public anxiety about perceived invasions of privacy.

The development of modern forms of social organization of increasing size and complexity and the corresponding growth of large public and private institutions have given rise to an unprecedented growth in the collection, analysis and use of information. This increase in institutional needs for information has been coupled with remarkable gains in the sophistication and capacities of technologies used in the gathering, storage, analysis and dissemination of information. It is often said, with good reason, that we are living in an "information age." Personal information concerning individuals is now collected and used by

large institutions to an extent that would have been inconceivable to previous generations.

We do not suggest that the growth of modern forms of social organization and the use of sophisticated information technology are developments to be deplored. Much of what is viewed as social and economic progress is intimately related to the growth of large organizations and their effective use of information and information systems. Indeed, these developments do not invariably have a negative impact on privacy. Modern urban social conditions permit an individual to retain a degree of anonymity which would be impossible in village life. So too the computer (perhaps the most feared of modern technological breakthroughs) may offer more privacy protection than information systems consisting solely of manually stored (and easily accessible and readable) files[5].

Clearly, however, these developments have brought with them the capacity for substantial disruption of our private lives. Further, as indicated in greater detail in Chapter 30 of this report, our existing framework of laws appears to be incapable of providing redress in situations where these risks of privacy invasion accrue. In his influential book, Privacy and Freedom[6], Alan F. Westin suggests that the protection afforded to privacy interests by the U.S. law of the late eighteenth and nineteenth centuries was adequate to meet the potential threats to privacy posed by contemporary social conditions, but that events (primarily technological innovations) have outstripped these controls in the last eighty or ninety years. In the earlier period, personal privacy was protected by laws guarding the property owner from unwarranted intrusion, ensuring the privacy of the mail, prohibiting eavesdropping and protecting the individual from unlawful search or seizure by public authorities. These and other privacy-supportive laws offered adequate protection from any potentially invasive methods of surveillance existing at the time.

In Westin's analysis, two waves of technological change occurred, to which the law failed to formulate an adequate response. The first period of change came at the turn of the century with the development of the telephone and sound recording technology, and the refinement of photographic equipment. The privacy-invasive surveillance capacities of each innovation were soon realized. Stories appeared in the press of the time indicating the use of wiretapping techniques and hidden microphones for the purpose of eavesdropping. Complaints arose about the use of cameras by private detectives, and about the unauthorized publication of photographs by advertisers and the press. Concern over the press coverage of the wedding of Samuel Warren's daughter led to the famous article written in 1890 by Warren and Louis D. Brandeis, "The Right to Privacy"[7].

The second and more recent wave of technological change occurred in the period following 1950. Westin describes a dramatic increase in sophistication and usage of three types of surveillance technology: physical surveillance by means of optical or acoustical "bugging" devices; psychological surveillance of polygraph analysis and psychological tests of various kinds; and data surveillance, or "the collection, exchange, and manipulation of documentary information about individuals and groups by data-processing machines (primarily computers)"[8]. It is this last innovation, the growth of data surveillance, which is of particular relevance to our inquiry.

Westin, writing in 1967, expressed the opinion that the "balance of privacy" which had been achieved in U.S. law in the nineteenth century had been dislocated by these developments, and that substantial legal intervention through the development of privacy protection laws of various kinds would be necessary to respond to these changed social conditions. Since that time, there have been substantial legislative initiatives taken in the United States, many of them similar to proposals advanced by Westin[9].

In the United States, federal laws controlling the use of electronic surveillance or wiretapping devices were enacted in 1968[10]. In 1970, the data-gathering and dissemination activities of the credit reporting industry were subject to control by the Fair Credit Reporting Act[11]. In 1974, legislation was adopted which granted rights of access to school records to students and their parents, ensured that an opportunity would be afforded to correct erroneous information, and limited the uses to be made of these records[12]. Finally, and of more direct relevance to our own mandate, in 1974 comprehensive regulation of the use of personal information by agencies of the federal government was introduced in the Privacy Act of 1974[13]. Similar developments have occurred in the United States at the state level[14].

Privacy protection legislation similar in its essentials to these U.S. developments has also been adopted in Canada at the federal and provincial levels, although not to the same extent. Controls over the use of electronic surveillance were adopted by the federal government in 1974 in the Protection of Privacy Act[15]. On March 1, 1978, the provisions of Part IV of the Canadian Human Rights Act[16] regulating the use of personal data by the federal government were proclaimed to be in force. In Ontario, legislation securing privacy protection rights with respect to school records was enacted in 1972[17]. Legal controls over the personal information practices of the credit reporting industry were enacted in 1973[18].

Ontario has not, however, adopted comprehensive legislation along the lines of the U.S. Privacy Act of 1974, or the Canadian Human Rights Act, Part IV. This Commission has been concerned to reach an opinion as to whether a legislative initiative of this kind is warranted in the context of the personal information practices of the government of Ontario.

In preparing the ground for recommendations on this matter, we have examined current Ontario law and government practices relating to the collection and use of personal information, as well as the experiences of other jurisdictions in North America and Europe which have adopted regulatory schemes controlling the handling of personal information by government authorities. Before turning to our account of these investigations, however, it will be useful to articulate the underlying definition of the privacy protection issue which has animated our inquiry.

B. DEFINING PRIVACY

An examination of privacy protection problems relating to government records in Ontario could only be attempted after reaching some consensus as to the nature of the privacy interest. This preliminary task is more difficult than it may at first appear. Indeed, volumes have been filled with learned articles by philosophers, jurists and other academic specialists attempting to fashion a rigorous definition of the concepts of "privacy" or "the right to privacy"[19]. It would be a rash and unnecessary gesture for this Commission to attempt to referee these academic disputes. Yet it is possible, we believe, to distill from these discussions and from our own appreciation of these issues common themes which point in the direction of a consensus as to both the meaning of personal privacy and the significance of the development of modern information systems for maintaining personal privacy.

It is difficult to develop a single comprehensive definition for a term commonly used to describe a variety of related states of affairs or conditions, and whose meaning therefore may alter slightly from one context to the next. Thus, it is helpful to isolate, in the manner suggested by the federal Canadian Task Force on Privacy and Computers[20], the different contexts in which claims of invasions of privacy may arise.

The task force identified and defined "territorial privacy," "privacy of the person," and "privacy in the information context" in the following terms[21]:

a. Territorial Privacy

Claims to privacy advanced in a territorial or spatial sense are related historically, legally and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquility is advanced and is recognized. A man's home is his castle. At home he may not be disturbed by trespassers, noxious odours, loud noises, or peeping Toms. No one may enter without his permission, except by lawful warrant.

b. Privacy of the Person

In a second sense, a claim to the privacy of one's person is protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person. This notion, like the territorial one, is spatial in the sense that the physical person is deemed to be surrounded by a bubble or aura protecting him from physical harassment. But, unlike physical property, this "personal space" is not bounded by real walls and fences, but by legal norms and social values. Furthermore, this sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. Our persons are protected not so much against the physical search (the law gives physical protection in other ways) as against the indignity of the search, its invasion of the person in a moral sense.

c. Privacy in the Information Context

The third category of claims to privacy was of primary relevance to the Task Force. It is based essentially on a notion of the dignity and integrity of the individual, and on their relationship to information about him.

This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. And this is so whether or not the information is subsequently communicated accurately, and whether or not it is potentially damaging to his reputation, his pocket-book, or his prospects; the context is of course the controlling factor in determining whether or not particular information will be damaging. Competing social values may require that an individual disclose certain information to particular authorities under certain circumstances (e.g., census information).

He may decide to make it available in order to obtain certain benefits (e.g., credit information or information imparted to his lawyer to win a lawsuit or to his confessor to win salvation). He may also share it quite willingly with his intimates. Nevertheless, he has a basic and continuing interest in what happens to this information, and in controlling access to it.

The essence of the notion of privacy appears to change as attention shifts from privacy in the context of physical isolation to privacy in the context of the processing of personal information by, for example, the credit reporting industry. Nonetheless it would be difficult to improve on Professor S.I. Benn's suggestion that the state of privacy is simply that of "not sharing an experience, a place, or knowledge with anyone else," or, where two or more people are enjoying a state of privacy together, "there is sharing only because the subjects want to share"[22].

Jurists have attempted to develop a satisfactory definition of the "right" to privacy and to offer a persuasive rationale for its assertion[23]. As early as 1888, U.S. Judge Thomas M. Cooley suggested that the right to privacy could be simply expressed as "the right to be let alone"[24]. Two years later, Warren and Brandeis argued that the legal system's tacit recognition of certain privacy rights was a recognition of a principle of "inviolable personality"[25]. Predictably, since that time, some legal writers[26] have criticized these attempts at the articulation of so vague or general a "right" and have attempted to cite instances in which specific rights of privacy have received recognition. Others[27] have attempted to reassert more general theories of the privacy right in an effort to reconcile divergent trends in the case law dealing with claims brought by individuals claiming damages for invasion of privacy[28].

When we turn to discussions of the right to privacy in the information context, however, a clearer consensus as to the nature of the privacy interest emerges. It seems that most writers who have addressed this aspect of the subject agree with the approach suggested by the federal Canadian Task Force that the essential concern of the individual is to maintain the right to limit the disclosure and subsequent use of information concerning himself. Professor Westin has defined privacy as "the claim of individuals, groups, and institutions to determine for themselves when, how and to what extent information about them is communicated to others"[29]. Similarly, Professor Miller has stated that the right to privacy is constituted by "the individual's ability to control the circulation of information relating to him"[30].

There is general agreement as to the social importance to be attached to the informational privacy claim. Professor Westin, among others, draws a line connecting privacy and personal autonomy or freedom, and identifies the concern to preserve individual freedom as a major justification for the recognition of a right to privacy[31]. Two aspects of personal autonomy are threatened by privacy invasions: our relationships with other individuals, and our relationships with institutions.

The importance of privacy in the context of interpersonal relationships has been examined in an illuminating manner by Charles Fried[32]. Having defined privacy as "the control we have over information about ourselves"[33], he goes on to suggest that the ability to grant or deny others access to such information is an element of personal liberty which enables the individual to control the context within which he acts. Such control over the informational context of one's actions is an essential prerequisite to many "significant ends in life," such as "love, trust, friendship, respect, and self-respect." For example, the ability to determine when, in what way, to whom and to what extent to communicate information concerning one's health plays an important role in enabling one to define relations of friendship or trust with another person. Indeed, in Fried's view, the importance of privacy for these purposes is absolute.

Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence. To make clear the necessity of privacy as a context for respect, love, friendship, and trust is to bring out also why a threat to privacy seems to threaten our very integrity as persons. To respect, love, trust, or feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion[34].

Though it may well be that so strong a claim cannot be made for all incursions on one's ability to control the flow of information concerning oneself, Fried's analysis may offer an explanation for the instinctive unwillingness of individuals to share sensitive personal data with strangers and the desire to control the flow of such information even to friends and intimates.

The surrender of control over personal information to institutions raises additional issues. Some element of the personal autonomy analyzed by Fried is present in this context. Institutions are staffed by individuals, and some of the public

resistance to the disclosure of sensitive personal information to institutions may rest on a desire to avoid disclosure to those individuals. But an additional concern arises from the fact that the information is usually gathered by the institution for the purpose of monitoring the activities of the individual or making determinations which may affect him. For example, credit reporting agencies maintain credit records in order to identify individuals who are not meeting their obligations consistently; these records are used by potential creditors in making decisions to grant or deny credit. Information is gathered by social welfare agencies to determine eligibility for benefits. Sensitive personal financial information is gathered by the taxing authorities in order to monitor compliance with the legal requirement to pay income tax. In short, as James B. Rule[35] has observed in a comparative study of British and U.S. institutional record-keeping systems, information is often gathered for the purpose of exercising some form of control over the conduct of the individuals about whom records are kept. The loss of control over personal information may, in this additional sense, be accompanied by a restriction in one's personal autonomy. This is not to suggest that such restrictions are unavoidable in contemporary society -- indeed, they may be the inevitable accompaniment of a beneficial social or economic measure -- but simply to note that a diminution of personal autonomy is a consequence of the growth of information systems employed in the decision-making and monitoring activities of large institutions.

In summary, then, the privacy interest that arises in the information context relates to the desire of individuals to maintain control over the disclosure and dissemination of information concerning themselves. The claim that such control should be maintained, to the extent possible in modern social conditions, is linked to fundamental concerns for the preservation of human dignity and personal freedom.

C. THE INFORMATIONAL PRIVACY ISSUE

In light of the foregoing discussion of the definition of "privacy," "informational privacy," it is not difficult to see why increasingly vocal concerns are being expressed about the threat to individual privacy posed by the growing use of "data surveillance" by large institutions. As the U.S. Privacy Protection Study Commission has observed:

The substitution of records for face-to-face contact in these relationships is what makes the situation today dramatically different from the way it was even as recently as 30 years ago. It is now commonplace for an individual to be asked to

divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are, or have come to be considered, necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make. Organizations must have some substitute for personal evaluation in order to distinguish between one individual and the next in the endless stream of otherwise anonymous individuals they deal with, and most organizations have come to rely on records as that substitute[36].

It would be naive in the extreme to assume that the currents of social growth and development which have brought with them the growth in the use of data surveillance could be turned back, even if such an objective were desirable. Nonetheless, the growth of this documentary world, of such great significance to the individuals whose lives are therein recorded, brings with it certain privacy "costs." If the preservation of informational privacy is to be fostered, these costs should be weighed in the balance when decisions are taken to increase the use of information technology, and they should be taken into consideration in the design of new information systems.

Several privacy costs may be identified. First, as indicated previously, an invasion of privacy results from the loss of control over the dissemination of personal information concerning oneself. This occurs both when the information is first surrendered and when subsequent use or dissemination of the information is made without the consent of the data subject. This invasion may be particularly acute where the information has been gathered from someone other than the data subject. Second, some observers have expressed concern that the growth of documentation creates a pressure to perform "for the record" with a consequent loss in personal autonomy. Third, the persistence of the paper record makes it more difficult for an individual to "make a fresh start," to resolve to conduct himself in new and more responsible ways and reap the benefits which might otherwise flow from such conduct. Fourth, the growth of decision making "by the record" increases the danger that the determinations will be made on the basis of erroneous information, with consequent unfairness to the individual.

The solution proposed by Westin to the informational privacy problem in 1967, and by many others since, is to subject the operation of personal data systems to some form of regulatory control and to develop mechanisms which would enable the individual to retain some measure of control over the dissemination of personal data, and to assert the right to challenge the accuracy of data

stored in information systems[37]. Much of the recent legislation referred to in the opening section of this chapter embodies these kinds of privacy protection mechanisms.

The Ontario Consumer Reporting Act[38] provides a useful illustration of this phenomenon. (This legislation is described in detail in Chapter 30 of this report.) In essence, the act imposes limits on the kinds of personal information that credit reporting agencies can gather and the period of time that it can be retained; it also enables the subject of a credit report to have access to the agency file concerning him and to protest the accuracy of the information therein, and requires that the individual be notified when information is sought by a potential credit grantor from a credit reporting agency. The legislation tacitly accepts the value of efficient credit reporting to the economic system. Indeed, it may do much to improve its accuracy and, consequently, its value to users, as well as its acceptability to the general public. At the same time, the legislation reduces the privacy intrusiveness of credit reporting by imposing limits on data collection and by ensuring opportunities for the individual to be aware of and to participate in the use of credit data, and, further, attempts to ensure the fairness of credit decisions by permitting the data subject to challenge the accuracy of the credit record.

The informational privacy issue involves striking appropriate balances between the organizational interest in the collection and use of personal information and the interests of the individual in reducing the intrusiveness of data collection, in participating in decisions with respect to subsequent use, and in ensuring fairness in decision making based on personal files.

D. POLITICAL DIMENSIONS OF THE ISSUE

The privacy problems associated with data surveillance gain a new dimension where the data-gathering activity is undertaken by the government. As Westin has pointed out, the history of the development of Western traditions of individual liberty and democratic institutions is replete with illustrations of limitations being imposed on the power of governmental authorities to engage in surveillance of the citizenry. It was Westin's thesis that "American society in the 1970s faces the task of keeping this tradition meaningful when technological change promises to give public and private authorities the physical power to do what a combination of physical and socio-legal restraints has denied to them as part of our basic social system"[39]. The use of data surveillance by government signals, in our political tradition, a concern that fundamental values relating to the integrity and

liberty of the individual are involved, and that care must be taken to ensure that those values are not seriously threatened or impaired.

Apart from this general concern that an appropriate balance be maintained in the relationship between individuals and their government, a number of more specific privacy-related concerns arise with respect to government data banks. First, the collection of personal information by government is not likely to occur in circumstances in which the individual has an effective choice of refusing to supply the information in question. Second, the broad range of government activity impinges on so many aspects of personal life that the extent of the total personal information holdings of the government vastly exceeds the amount which could conceivably be collected by any single private organization. Further, there is some public anxiety about the prospect of government ministries and agencies engaging in data sharing or data linkage -- drawing personal information from a variety of government data banks and building comprehensive personal files or dossiers on individual citizens. Indeed, the development of substantial public concern with respect to the privacy issue in the United States is attributable, in part, to the proposal in the mid-1960s to establish a National Data Center which would have linked personal files held by federal government agencies in this way. After prolonged congressional investigation of the proposal, the scheme was abandoned[40]. Much of the concern expressed by Canadians with respect to the increasing use of the Social Insurance Number as an identifying characteristic in personal files reflects this fear of dossier building[41]. Finally, the economic and public relations implications of intrusive data surveillance may provide more effective disincentives to its use by business organizations than to its use by government[42].

Important as the informational privacy value is, it is but one of a number of potentially conflicting values competing for attention. The government must gather personal information if it is to successfully and efficiently administer the social and economic programs adopted in response to its perceptions of the public interest; if we are to have a government-operated medical insurance scheme, for example, it is inevitable that some personal information-gathering activity will occur. Similarly, concern about the use of surveillance technology by law enforcement authorities must be measured against the need for effective law enforcement. The potential dangers in the use of numerical identifiers such as the Social Insurance Number must be weighed against the desirability of accurate identification of records concerning individuals and the possible benefits of personal data linkage for medical research purposes. Further, as we have been at pains to indicate in this report, informational privacy values

must compete with the freedom of information interest. Public servants may have reservations about displaying their work product or the details of their employment contracts to the public; these must be measured against the public's interest in being able to effectively scrutinize the conduct of public affairs. In short, the informational privacy value is not absolute; it must be measured against and reconciled with competing public goods.

As others have suggested, however, it is well to note that the privacy value may be particularly vulnerable to submersion in political decision-making processes; in any particular case, the arguments for engaging in data surveillance are likely to be considered to be more immediate and compelling than what may appear to be the more abstract and philosophical concerns underlying the information privacy interest. As S.I. Benn has written:

...privacy is a particularly vulnerable interest; in any given case, it is the interest of one individual or a relatively small group, while against it are set the interests of the public in being fully informed, in security from crime, in having policy-makers and administrators of the national economy, or [the public health insurance scheme] or city plans work with full and up-to-date information. Consequently, in any given instance, the public interest will seem overriding; yet in the long run protection of the interest of every individual in privacy will have gone by default; the piecemeal erosion of the privilege may never have been halted, to take an overall view of the total consequences. In this respect privacy resembles environmental values; the particular damage rarely seems sufficient to outweigh the promised benefits, but the cumulative consequences may be disastrous[43].

As will be seen, it is not the Commission's view that the personal record-keeping practices of the government of Ontario have approached this disastrous state of affairs. Nonetheless, the desirability of maintaining a general perspective on the growth of personal record keeping is a theme to which we shall return.

E. PRINCIPLES OF FAIR INFORMATION PRACTICES

In various North American and European jurisdictions, a consensus has emerged with respect to basic principles of fair information practice. If followed, the principles should result in the realization of some individual control over the personal information collected and used by institutional record keepers.

The principles were first clearly articulated in the well-known and influential report of a committee of the U.S. Department of Health, Education and Welfare[44]. Published in 1973, the report stated the "fundamental principles of fair information practice" in the following terms:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using or disseminating records or identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data[45].

The basic philosophy expressed in these principles, coupled with a concern to restrain excessive data gathering, is evidenced in government reports, statutes and proposed legislation in most technologically advanced Western societies including Canada, the United States, Australia, and the eighteen member countries of the Council of Europe. The principles have been cast in statutory language and in guidelines, and have been used as a base against which to measure the progress of governments and other institutions in responding to informational privacy problems. Frequent reference will be made to these principles in the body of this report.

F. PUBLIC OPINION

Attempts have been made in recent years to measure public attitudes toward privacy protection issues. Public opinion polls conducted in North America and Great Britain indicate that citizens are indeed worried about the general proliferation of personal records, the tendency of government to store and disseminate personal information, the use of computers in record keeping and the corresponding loss of personal privacy. In 1970, a poll conducted by Louis Harris Associates found that 34 per cent of the

U.S. public felt their sense of privacy was sometimes invaded. Harris polls have, over the past ten years, revealed a mounting public concern about loss of privacy and an increasing tendency for Americans to blame organizations such as government for invasive record-keeping practices. (See Table 1.)

Table 1

	1970	1974	1976	1977	Jan. 1978	Dec. 1978
Concerned with threats to personal privacy	34%				47%	64%
Believe that "organiza- tions and agencies ask you for too much infor- mation"			33%	59%		72%
Feel threatened by having personal information about them on file		23%		32%		

Sources: Kentucky Legislative Research Commission, Personal Information and Privacy (Lexington: Legislative Research Commission, 1978) 9-10; Louis Harris and Associates, The Dimensions of Privacy (Stevens Pt., Wisconsin: Sentry Insurance, 1979) 14, 22.

To document these trends, Louis Harris Associates and Dr. Alan F. Westin conducted an exhaustive national privacy survey for the Sentry Insurance Company in December 1978[46]. The pollsters discovered that 50 per cent of Americans now worry about how the federal government will use information it collects about them; about one-third feel that taxing authorities (the Internal Revenue Service), intelligence agencies (The Central Intelligence Agency and the Federal Bureau of Investigation) and government welfare agencies "ask for too much personal information"; a substantial percentage (ranging from 41 per cent to 26 per cent depending on the agency) feel government operations should be doing more to keep information they have on individuals confidential. In reference to technological concerns, public perceptions of the computer as a threat to privacy have risen markedly (from

37 per cent to 54 per cent) since the 1976 Harris poll. It was evident from the results of the survey that Americans favour strong action, including legal protections, to address privacy problems.

Although not designed to canvass opinions about informational privacy, a poll conducted in 1971 for the Younger Committee[47] provides some insight into British attitudes about privacy and record keeping. The majority of respondents (58 per cent) felt that "people have less privacy than they used to have." The main reason given for the decline of privacy was an increase in the number of forms to fill in and a consequent feeling that "too much is known about you by a wide variety of organizations." The notion of a central computer, in which "details of your life such as family circumstances, financial situation and political views, with any of the information being available to anyone who asks for it" was repugnant to 87 per cent of the respondents, almost all of whom felt such a facility should be prohibited by law. On the other hand, few objected to publication of personal details about themselves such as address, telephone number, nationality, race, occupation, education or religious views. Strong objections were registered only to the publication of "details of sex life," income, political views and medical history. In contrast to U.S. studies, the British study concluded that "the public's feelings about privacy that emerge from this survey are those of concern and apprehension rather than a demand for immediate action."

Canadian viewpoints on privacy and record keeping have not been periodically assessed. However, a survey conducted for the federal Department of Communications indicated a public skepticism about the impact of growing computer use on privacy as early as 1972[48]. In that poll, 52 per cent of respondents agreed with statements that "computers are reducing people to just numbers"; 69 per cent felt that computers cause errors because they cannot "take human factors into account"; 37 per cent felt that "computers threaten our personal privacy"; and 52 per cent felt that "computers will cause violations of confidentiality." An analysis of the survey concluded that "in general, there would appear to be a higher degree of pessimism and a lower degree of optimism about the use of computers in Canada than in the United States." The survey did not solicit opinions about the merits of various possible solutions to privacy problems.

The Commission did not feel that it would be a useful expenditure of public funds to engage in extensive and expensive polling of public attitudes in Ontario. Rather, our approach was to attempt to discern whether current law and practice in Ontario warrants public concern, and, more particularly, the adoption of a new government policy relating to the protection of individual

privacy. Nonetheless, it is of interest that polls conducted elsewhere confirm our expectation that public attention is increasingly directed to the privacy protection issue.

G. AREAS OF CONCERN

In approaching the task of examining current Ontario government practice with respect to the collection, use and dissemination of personal data, the Commission identified the following areas of potential concern[49]:

PUBLIC KNOWLEDGE OF PERSONAL DATA BANKS

Public knowledge of the existence of personal data systems is considered by many to be of fundamental importance to the protection of informational privacy, especially in the context of government records. Public knowledge of the nature and use of government-held personal information banks is presumed to be instrumental in preventing undue government intrusion into or control over the lives of citizens. Accordingly, we have attempted to determine the extent of public knowledge of these activities in Ontario.

COLLECTION OF PERSONAL INFORMATION

Recognizing that individual privacy is first endangered at the point of collection of sensitive personal data, we have attempted to identify current policies and practices regarding what, how and from whom personal information is collected and verified. We have examined the collection of such data items as standard identifying numbers (for example, the SIN), subjective judgmental data, and other sensitive personal data used in decision making or in the administration of government programs; we have considered the issues of voluntariness of record subjects in supplying information and the protection of privacy during the information-gathering process; and we have looked at the gathering of data about a record subject from people or organizations other than the subject.

MAINTENANCE OF DATA INTEGRITY AND SECURITY

The adequate safekeeping of personal data is as important to the protection of the privacy of record subjects as is the method of gathering the data. Record storage practices designed to prevent loss, misplacement and unauthorized use of personal

information, and to ensure that old or irrelevant data are not used against record subjects, have been examined. Other significant concerns are the physical security of record holdings, information storage and retrieval methods, destruction of old or irrelevant records, the existence of policies determining retention periods for data, and procedures for disposing of stale or irrelevant data.

TRANSFER AND DISSEMINATION OF PERSONAL INFORMATION

The transfer of information between a subject's original record at one location, and any other person, office or agency signals a further loss of subject control over the use and dissemination of that information. For this reason, attention was devoted to the extent and types of personal information transfers, the nature of subject awareness of and authorization for such transfers, and the uses made of government-held data by third parties.

SUBJECT ACCESS TO PERSONAL RECORDS

The granting of access to personal files by the data subject, in order to enable him to check the accuracy, relevance and uses made of information about him, is considered by many observers to be a central element in the protection of individual privacy. The record subject is the person most likely to be negatively affected by government decisions made on the basis of subjective or incorrect data, by poor maintenance techniques, and by unauthorized transfers of information between record holders. We have attempted to discover the extent to which subject access and correction rights are recognized in current practice.

COMPUTERIZATION OF PERSONAL RECORDS

Informational privacy concerns are intensified by the increasing use of sophisticated computer technology. We have examined the extent of the current use of computers, and the implications of the rapid growth in the information processing capacities of a technology which appears to enjoy a sustained and unpredictably rapid improvement. Our discussion of these issues is to be found in the next chapter of this report.

CHAPTER 25 NOTES

- 1 See, for example, I.C. Velecky, "The Concept of Privacy" in J.B. Young, ed., Privacy (Toronto: John Wiley and Sons, 1978) 15-17, cited hereafter as Young.
- 2 A.F. Westin, Privacy and Freedom (New York: Atheneum, 1967) 11-18, cited hereafter as Westin; John M. Roberts and Thomas Gregor, "Privacy: A Cultural View" in J.R. Pennock and J.W. Chapman, eds., Privacy (New York: Atherton Press, 1971) 199-225, cited hereafter as Pennock and Chapman.
- 3 Westin, 8-11; P.H. Klopfer and D.I. Rubenstein, "Privacy and its Biological Basis" (1977) Journal of Social Issues 52.
- 4 This theme is explored by D.N. Weisstub and C.C. Gotlieb in "The Nature of Privacy," a background study prepared in 1972 for the Canadian Department of Communications/Department of Justice Task Force on Privacy and Computers. An extensive investigation of the significance of privacy in American colonial life has been undertaken by Professor D.H. Flaherty; see Privacy in Colonial New England (Charlottesville: University of Virginia Press, 1972).
- 5 The privacy protection implications of the use of computer technology are considered in Chapter 26 of this report.
- 6 See generally, Westin, Chapter 13.
- 7 (1890) 4 Harv. L. Rev. 193. The historical point is noted by H. Kalven Jr. in "Privacy in Tort Law -- Were Warren and Brandeis Wrong?" (1966) 31 Duke L.J. 326.
- 8 Westin, 98.
- 9 Westin's book, together with Arthur R. Miller's The Assault on Privacy (Ann Arbor: University of Michigan Press, 1971), cited hereafter as Miller, and the report of the Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens appear to have been major influences on contemporary U.S. privacy protection policy.
- 10 The Omnibus Crime Control and Safe Streets Act of 1968 (Title III), Pub. L. No. 90-351, para. 802, 82 Stat. 212.
- 11 15 U.S.C. s. 1681, Pub. L. No. 91-508.
- 12 Family Educational Rights and Privacy Act of 1974, 20 U.S.C., s. 1232g.

- 13 5. U.S.C. 552a.
- 14 For a useful compendium of privacy related laws, see R.E. Smith, Compilation of State and Federal Privacy Laws, 1978-79, published annually by the Privacy Journal, Washington, D.C.
- 15 S.C. 1973-74, c. 50.
- 16 S.C. 1976-77, c. 33.
- 17 An Act to Amend the Schools Administration Act, S.O. 1972, c. 77, s. 14.
- 18 The Consumer Reporting Act, S.O. 1973, c. 97.
- 19 See, for example, Pennock and Chapman; Young.
- 20 Canada, Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972), cited hereafter as Privacy and Computers.
- 21 Ibid., 13-14.
- 22 S.I. Benn, "The Protection and Limitations of Privacy" (1978), 52 Australian Law Journal 601 at 602, cited hereafter as Benn.
- 23 For a useful account of many of the attempted definitions, see D.M. O'Brien, Privacy, Law and Public Policy (New York: Praeger, 1979).
- 24 Thomas M. Cooley, Treatise on Torts (2nd ed., 1888).
- 25 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890), 4 Harvard L. Rev. 193.
- 26 See, for example, W.L. Prosser, "Privacy" (1960), 48 California Law Review 383.
- 27 See, for example, E. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964), 39 New York University Law Review 902.
- 28 An account of Canadian common-law doctrines relating to privacy protection appears in Chapter 30 of this report.
- 29 Westin, 7.
- 30 Miller, 25.

- 31 Westin, 33-34.
- 32 Charles Fried, An Anatomy of Values (Cambridge: Harvard University Press, 1970) Chapter 9.
- 33 Ibid., 140.
- 34 Ibid.
- 35 James B. Rule, Private Lives and Public Surveillance (New York: Schocken Books, 1974).
- 36 Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington: USGPO, 1977) 4-5.
- 37 Westin, Chapter 4.
- 38 S.O. 1973, c. 97.
- 39 Westin, 22.
- 40 For an account of this proposal and its fate, see Miller, 71-82.
- 41 See, further, Chapter 28 of this report.
- 42 A similar observation is made in the New South Wales Privacy Committee Report 1975-78 (Sydney: Privacy Committee, 1978) 8.
- 43 Benn, 691.
- 44 The Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens (Cambridge: Massachusetts Institute of Technology, 1973).
- 45 Ibid., 41.
- 46 Louis Harris and Associates, The Dimensions of Privacy (Stevens Pt., Wisconsin: Sentry Insurance Co., 1979).
- 47 Great Britain, Report of the Committee on Privacy (1972; Cmnd. 5012) 232, 238-40, 254-57.
- 48 Social Survey Research Centre of Toronto, Survey of Public Attitudes Towards the Computer (Ottawa: Department of Communications, 1973) 5-10, 18.

49 A similar list of issues was addressed in Privacy and Computers, 16.

Computers and Privacy

A. THE COMPUTER'S EFFECT ON PRIVACY[1]

Although government agencies, like all large organizations which deal with people, have always collected personal information, the relatively recent widespread use of computer-readable files has triggered controversy over the privacy and security of these records. In the popular imagination, the computer has been seen as the villain of the piece because it greatly increased the capacity of governments to store, manipulate, analyze, and communicate large amounts of information. This, in turn, raised the spectre of a society in which every significant act or transaction of an individual would become a matter of public record or concern. In addition, fears were expressed that computer-held records were vulnerable to unauthorized or illicit access and use.

Expert opinion on the extent to which computer-based technology, in and of itself, represents a distinct threat to the fabric of democratic society is divided. There is no doubt that the simple existence of an information storage and retrieval tool as powerful as a modern computer greatly increases the capacity of government to use, for good or ill, the information which it collects. However, the chief effect of computerization has been to increase government efficiency in the handling of personal data. The gathering of data is still largely done by non-electronic means which are expensive and time-consuming. Moreover, public policy decisions to assemble detailed dossiers on ordinary citizens or specific groups and to track significant acts or transactions of certain individuals have been taken in countries where the use of such technology is not widespread, such as the Soviet Union, parts of Latin America, and the Middle East. At the very least, this would suggest that computerization and the autocratic use of personal information do not necessarily go hand in hand.

Another source of popular concern has been the apparently exponential increase in the adoption of computer-based technology by retail companies, banks, public utilities, insurance companies, and other private sector organizations during the past twenty years. Controversies regarding the computerization of these records have frequently reflected a fear that they might be used by private, governmental, or quasi-governmental agencies for

surveillance purposes or to deny individuals access to employment, credit, and other benefits.

While there has been general agreement that there are no insuperable technological barriers to these kinds of uses of computerized data files, there is little evidence of movement in this direction at present. A study conducted by Alan Westin of fifty-five U.S. governmental, commercial, and non-profit organizations in 1972 concluded that:

Computer usage has not created the revolutionary new powers of data surveillance predicted by some commentators. Specifically, the great majority of organizations we studied are not, as a result of computerizing their records, collecting or exchanging more detailed personal information about individuals than they did in the pre-computer era. They are not sharing identified information more widely among organizations that did not carry out such exchanges in the pre-computer era[2].

Westin cites four characteristic impediments encountered in the integration of data systems within and between organizations:

- a. the need to reorganize bureaucratic structures in order to fully utilize computer-based technology;
- b. the necessity for a clear articulation of the goals, programs, and decision-making patterns within an organization and the design of its data system;
- c. the high marginal cost of implementing new computer systems while continuing to gather and use data in a more traditional fashion;
- d. the divergent programming requirements of different potential users of central data banks[3].

Two primary constraints still impede the integration of data systems within and between organizations: organizational, or having to do with the necessity for bureaucratic reorientation in order to accommodate the new technology, and socio-legal, or having to do with explicit restrictions on data sharing. Moreover, the clear thrust in research, particularly since 1974, has been in two directions: further adapting technology to existing organizational arrangements (thus minimizing the disjunction between bureaucratic structures and the technical requirements of data processing) and detailed study of the ways in which computer-based technology can be most easily introduced into the work environment[4].

To fully grasp the broader implications of these developments for individual privacy, it is useful to review the history of computerized data processing in general, and in particular, to consider how this has affected the way in which personal records have been dealt with by governments and other large-scale organizations.

B. THE DEVELOPMENT OF COMPUTER SYSTEMS

In recent years, there has been a marked growth in both the "hardware" and "software" capabilities of computer systems[5]. Initially, computers were simply used to improve the efficiency of repetitive clerical operations, such as accounting and payroll, which had previously been performed by electro-mechanical devices employing punch card input. At this point, a large number of functions associated with computerization of data were still performed manually and computer time itself was not used efficiently.

In the early 1960s, larger machines and machine systems greatly extended the amount of active core available to a user, and processing time was greatly reduced as speed improved. Large organizations began to automate their high-volume service activities such as retail credit transactions, lists of customers, bank statements, insurance claims, and lists of motor vehicle drivers. The development of time sharing (the sharing of active workspace by multiple users) allowed for much improved machine efficiency and made central data processing centres accessible from remote terminals. Improved data storage allowed for on-line processing of data which could be automatically called up by the user. These developments, in turn, facilitated the use of computers as a locus for the actual storage (as opposed to processing) of data, and made it economical to use computers to retrieve relatively small amounts of information stored within much larger files. Software developments (the creation of powerful new languages such as APL for on-line use, and improved text-handling capabilities) kept pace.

By 1970, the stage was set for two important changes in the technological basis of computerized record keeping. The first of these arose from the creation of multi-purpose software "shells," called data base management systems (DBMS), which were flexible enough to store apparently unrelated information for a variety of similar uses. Coupled with earlier advances in hardware design, these systems greatly extended the forms of access to stored data[6]. This increased flexibility greatly extended the potential use of computer systems for non-operational purposes such as management, planning and modelling. The introduction and

increased commercial availability of inexpensive silicon chips led, in turn, to the creation of "intelligent" terminals[7]. Improved data communications also allowed for the efficient transfer of electronically gathered data from remote terminals and their flexible storage and analysis, on-line, by a variety of users. As a consequence, by the late 1970s, it was technically feasible to gather data, at source, electronically (for example, to enter transactions in a cash register); process the data locally using intelligent terminals or microcomputers; transmit the data to a central data processing centre; enter the data into a DBMS; and provide ready access to random pieces of information (such as the name of a customer who bought a clock radio on a certain day) or elaborate calculations based on the data (such as projected clock radio sales for the year). This access was available to relatively unsophisticated users virtually instantaneously.

The second important change in computer technology was the development of relatively inexpensive word processing devices and software systems[8]. In effect, given sophisticated programming, it is possible that, within a few years, the traditional line between "computerized" and "non-computerized" information will become almost completely blurred. Since the cost of such word processing systems is decreasing, and their capabilities are increasing, it is quite likely that they will become accessible to even small organizations in the near future.

While the adoption of this new technology by Canadian governments has been relatively slow to date -- a 1972 federal study rejected the notion of serious invasions of informational privacy arising at that time from computerization[9] -- earlier technical and organizational impediments to such invasions are likely to disappear or be greatly diminished. Moreover, restricted government budgets and rising civil service wages may act as a further incentive for the introduction and intensive use of existing technological capabilities. Under these circumstances, the fact that violations of informational privacy do not seem to have been widespread in the recent past is no guarantee that they will not become so in the near future. Moreover, while technological forecasting is far from an exact science, it seems reasonably clear that we can look forward to more communications being generated in electronic form; an increase in the ability of computer systems to analyze, store and retrieve text from documents; easier linkage of remote data systems; and easier access to data by those with little or no formal training in computer use. These trends suggest that a conscious effort is needed to ensure that informational privacy is maintained.

C. SECURITY OF COMPUTERIZED RECORDS

These continuing developments in the capabilities of computer systems make a serious examination of the security of computerized records imperative. Two related problems are apparent:

- a. the security of these systems against penetration by "outsiders," or those without authorized access to the system; and
- b. the security of these systems against unauthorized use of data by "insiders." (In this case, a further distinction needs to be drawn between unauthorized use for personal gain, and for bureaucratic purposes.)

Expert opinion has consistently concluded that

- . no computer system is perfectly secure;
- . time sharing greatly increases the likelihood that computer systems will be penetrated by outsiders;
- . the greater danger lies in the unauthorized use of data by insiders, not outsiders;
- . off-line storage of data limits access and, hence, unauthorized use;
- . restrictions on access to data are more likely to increase security than are restrictions on access to the machine itself.

If we distinguish, for the moment, between machine security (the ability of a system to impede unauthorized access to its hardware) and file security (ability to protect stored information) these issues will come into clearer focus. Machine security largely depends on the codes used in gaining access to the system. Since early computer systems did not store data in direct access (completely automated) files, these codes were initiated to account for and charge computer time to a given user. Because of a number of disadvantages inherent in the codes themselves and in recent computer developments which weaken the codes' abilities to protect machines, codes are no longer considered adequate barriers to illicit computer access[10]. A more reliable way of increasing machine security is to control access to the terminals through which the machine can be addressed. High security systems usually are "hardwired" (directly connected to the machine by a special "dedicated" line, rather than coupled through public telephone lines) in order to lessen their vulnerability. Once again,

however, this method of control is far more effective in preventing unauthorized access by outsiders than by insiders.

There is a general recognition that the crux of the problem lies in file security rather than in machine security per se. If someone has successfully entered a machine, there are a number of technical impediments which may be placed in his way in order to maintain record security[11]. In addition, the development of "distributed data bases" may reduce the problems associated with file security. Access to some of the information stored in a series of remote locations is allowed, but other classes of information are not shared. The advantages of centralized data processing are retained, but the difficulties involved in protecting a large centralized system are lessened.

Even where technical barriers to unauthorized use have been constructed, however, there are still a number of ways in which insiders or outsiders can gain unauthorized access to confidential information. Because the data being extracted from a machine is manipulable, it is quite possible for a user to gain access to bodies of information which do not, in themselves, disclose personal information or breach confidentiality, but which, taken together, may do so[12]. The potential for data combinations militates in favour of highly centralized systems where the combined use of data files can be more effectively monitored.

While it is relatively easy to establish procedures which will be successful in deterring those who would fuse related data from separate data banks for personal gain, it is not as easy to limit their use for bureaucratic purposes, even where these have been deemed to be beyond the scope of government activity. In the final analysis, only the establishment of firm policies on disclosure of data, a carefully planned system of internal controls, and auditing of data usage will succeed in limiting incursions of this kind.

D. TECHNOLOGICAL CHANGE AND PRIVACY

Computer technology is developing at such a rapid rate that it is difficult to forecast the directions in which it will turn. Predictions premised on "technology now known and understood" may, of course, be swept aside by the occurrence of as yet unforeseen technological breakthroughs. At present, pressures on information managers to maximize efficiency and minimize expense contribute to the reduction of privacy invasion[13]. But cost disincentives are rapidly disappearing as a factor in information systems planning (due, in large measure, to silicon chip technology). Similar technological developments will no doubt continue to expand the

capabilities and lower the costs of computer systems in the future. It is clear that no purely technological safeguards to the security and protection of privacy in computerized record keeping are likely to be effective in the long term.

E. AUTOMATION OF PERSONAL RECORDS IN THE ONTARIO GOVERNMENT

Most of the personal records systems maintained by the Ontario government examined by the Commission's research staff are, in fact, simply automated versions of the pre-existing manual records -- with little change in either the form or content of the stored data. In all the cases examined, some sort of manual system remains in place to provide a "hard" (non-electronic) record of the original or "source" document. In some instances, documents are microfilmed to reduce storage costs and the originals are then destroyed. Computerization has not increased the amount of data collected and maintained on file, but rather has allowed the data to be more rapidly and intensively used.

Most of the information collected by Ontario government agencies is used in the direct day-to-day administration of their various programs. Computerization can also aid in compiling statistics and producing reports. In some instances, this has been a deciding factor in a given ministry's decision to convert to automated storage and retrieval of its records. However, costs have proved to be an effective barrier, under present circumstances, to the development and use of computer systems solely for planning purposes. Thus, the thrust of program management within Ontario government agencies has been toward improving the operational efficiency and effectiveness of existing systems, rather than toward the proliferation of new data management activities. No central data bases have been created to which multiple users in different ministries have access. There is, however, sharing of information among different ministries and agencies -- some of this via remote terminals[14].

To understand the extent of automation of personal records by the Ontario government and the implications of computerization upon the privacy of Ontario citizens, two recent studies were reviewed. In 1976 a special task force appointed by Management Board of Cabinet identified 117 government-operated computerized data systems which contain personal information. Of the 117 Ontario government systems, 83 per cent were (or were intended to be) housed in one of three government computer centres. An additional ten such systems were implemented on ministry-owned mini-computers, and nine were operated through private service bureaus. The Ontario governments data centres are operated by the Computer Services Division, Ministry of Government Services, which:

provides computer services in support of the operational programs and service-delivery functions of ministries and agencies of the Ontario government[15].

The division consists of three separate computing centres[16] located in the Toronto area, and the Computer Support Services Branch. Each of the computing centres is predominantly used for operational or administrative data processing. However, each centre, to some extent, performs a full range of data processing functions.

In 1976, the special task force appointed by the Management Board of Cabinet examined the adequacy of privacy protection and security in the information practices of nine ministries. The study concluded that, while there was little evidence of information privacy violations, the potential for violations of both machine security and file security was "large and growing." While the task group reported that the responses to its questionnaires indicated that such security was, in general, reasonably good, it did note serious difficulties in the machine security arrangements and data-handling practices at one centre and in the operating practices of another[17].

In 1978, the Management Board of Cabinet commissioned a further study which, among other issues, examined the security of one data centre in detail. The consultants who carried out the study concluded that physical security and systems control in the data centre were adequate[18]. The systems integrity portion of the study again noted that security procedures for eight systems examined were also generally adequate. However, the need for security in individual ministry data preparation areas was indicated by the fact that over half of the systems allowed for remote terminal data entry. There are no overall standards for systems security within the Ontario government beyond those stated in the Manual of Administration:

ONTARIO MANUAL OF ADMINISTRATION, Section 55.2.5

Security of Systems

In order to ensure that operational systems and master files are secure from destruction because of errors and acts of vandalism or nature, the following minimum standard practices shall be followed:

1. Primary responsibility for the security of master files and data shall rest with the user.

2. All programs shall have up-to-date duplicates, and master files shall have back-up data in a form so that up-to-date master files may be easily and quickly recreated.
3. One complete set of up-to-date source programs and back-up data in a form so that up-to-date master files may be easily recreated shall be kept in a building other than the one where operating programs and files are processed. This off-site storage shall be in a secure and restricted area under government control.
4. Procedures shall be developed for the transfer and storage of data for each system dealing with confidential data. These procedures shall be approved by the responsible Branch Director or the responsible Division Executive Director. Also, in the case of systems with financial implications, the responsible financial officer shall approve the procedures.
5. Data processing centres shall develop procedures dealing with security of the facilities of the data centre, including restrictions on movement of personnel in the data centre.
6. Records retention arrangements shall reflect the requirements of the Vital Records Guidelines issued by Management Board.

Although many Ontario government personnel data files pass through or are stored in one of three large data centres operated by the computer services division of the Ministry of Government Services, this does not mean that these data are, necessarily, being cross-shared or amalgamated into one file. Information may be processed or stored in a data centre but the data systems, their operations and their storage are kept totally separate. Data centres typically have elaborate provisions to ensure that only authorized processing or data transfer occurs -- between as well as within offices. The consultants' report to Management Board notes that the measures employed by these centres are adequate at present. The Commission itself was unable to conduct an independent inventory of these security measures.

F. SUMMARY

While the nightmare of an environment in which every significant act or transaction of a citizen is open to government scrutiny has not materialized, important technological barriers to

the creation of such an environment have been or are being eliminated. Moreover, given recent software developments which have had the effect of adjusting computer systems to bureaucratic practice -- rather than vice-versa -- significant organizational barriers to the introduction of new computer technology have also been lowered. These changes -- together with the possibility that in the near future there is likely to be an almost exclusive use of computerized word processing systems for generation of written communications -- will certainly impact upon individual privacy. To mitigate this impact, it is imperative that we seriously consider socio-legal constraints which may be effective in reducing the possibility of computer-assisted abuses of privacy.

At the moment, there is no evidence that data processing or personal record keeping by the Ontario government is such that deliberate or systematic misuse of files by the Ontario government is going on. As yet, little sharing of data between agencies via computer links has taken place and no large integrated data banks have been created[19]. On the basis of the information we have at present -- but recognizing that we were unable to examine this issue directly -- it appears that both machine security and file security, while not perfect, are adequate for the short term. On the other hand, it must be stressed that no computerized record system is absolutely secure and any system, given the will and the resources, can be penetrated. Moreover, even if record systems and hardware currently in use were perfectly secure, new technological developments could render those security arrangements obsolete rather quickly.

Developments such as these, and some ministry plans for systems integration, highlight the need for a continual review of procedural and machine security standards by a professional task force without operational responsibilities for the direct day-to-day administration of government record-keeping systems. At present, no such group has been charged with data protection responsibilities in Ontario.

CHAPTER 26 NOTES

- 1 Material in this chapter is drawn largely from M. Brown, B. Billingsley and R. Shamai, Privacy and Personal Data Protection (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980) cited hereafter as M. Brown, 34-64, to which Dr. Stephen D. Berkowitz of the University of Toronto made extensive contributions.
- 2 Alan Westin, Databanks in a Free Society (New York: Quadrangle, 1972) 341.
- 3 Ibid., 238-40. Two of these impediments have been largely removed through technological advances which have occurred in the period since Westin concluded his study. The cost of implementing new computer systems has been greatly reduced through the introduction of prepackaged systems built to accommodate widely divergent intended uses. Moreover, the most advanced systems of this kind have been designed so that they can be accessed by persons with only minimal programming skills. In these cases, it is not necessary to "program" a computer; one need only select from a set of options which have been established in advance. In effect, then, the user is actually throwing "switches" in a program which already exists, not creating a program from scratch.
- 4 These two areas of inquiry -- the first largely conducted by computer scientists and the latter by social scientists -- have explicitly come together in an interest in how data base management systems can be addressed through the use of "natural language." This problem is clearly laid out in a now famous paper by E.F. Codd, "Seven Steps to Rendezvous with the Casual User," IBM Research Paper RJ1333 (#20842), 1974, dealing with so-called "casual users," i.e., those with a minimum of computer skills whose use of a system is episodic or irregular. Codd describes a means whereby systems may be created such that no previous experience with their organization or design and no programming skills are necessary in order to extract the information they contain.
- 5 "Hardware" refers to the mechanical devices for taking in (inputing), storing, retrieving and analyzing data; "software" refers to the sets of instructions (programs) which determine how these tasks are carried out. (For a fuller explanation of how computers work, see M. Brown, 40.)
- 6 For instance, data could be stored in "live files" and directly acted upon by users -- on-line query, on-line

response; data could be queried on-line, but large data processing jobs (especially those involving large amounts of printing) could be undertaken later -- on-line query, off-line response; queries could be entered off-line but results could be transferred to an active file; and queries could be entered and responded to off-line.

- 7 An intelligent terminal is a communications device which also has its own data processing capabilities. It is, in effect, a small computer, which can be used to preprocess data directly from a remote data-gathering device, thus eliminating the need for extensive data encoding and checking.
- 8 From the point of view of a low-level user, such systems have the advantage that a corrected (edited) draft can be printed directly, without the necessity for further correction or retyping. More sophisticated users can use the systems to analyze and monitor outgoing communications; monitor the productivity of clerical staff; create individually-addressed form letters or other standard forms where only name and certain details vary; and transfer natural language input into instructions for easy manipulation by a DBMS.
- 9 Canada, Departments of Communications and Justice, Computers and Privacy (Ottawa: Information Canada, 1972) 182, 184.
- 10 For a full explanation of codes, and their advantages and disadvantages in protecting access to computers, see M. Brown, 47-50.
- 11 For examples of such impediments, see M. Brown, 50-51.
- 12 For example, assume that a government insider could gain legitimate access not only to the date of birth, sex, and occupations of persons in a given area of a city and to a detailed list of the billings by physicians located in that area, but also to the date of birth of those physicians and their specialties. It may be possible to cross-match those physicians, calculate their incomes by applying the appropriate weightings for billing purposes, and retrieve a list of patients for each of them.
- 13 To the extent that the collection and storage of information creates significant costs, it is sound management policy to reduce data collection to the minimum necessary for the purposes in question and to destroy data whose storage costs exceed their value. Similarly, in part as a result of the cost involved, the conversion of manually-stored data to computer storage has proceeded less rapidly than early

observers predicted. Although the spectre of widespread linkage of existing data bases has given rise to considerable anxiety, the expense involved in accurate linkage of personal data from one data bank to the next has, in some measure, restrained the integration of computer records.

- 14 Motor vehicle files in the Ministry of Transportation and Communications can be directly queried by police through a mini-computer linked to a provincial communications network and to the Canadian Police Information Centre (CPIC) in Ottawa. This illustrates how communication systems can provide some of the efficiency associated with a central data base while allowing specific agencies to preserve control over their records. In this particular instance, there was no need to amalgamate files.
- 15 Ontario Ministry of Government Services, Annual Report for Fiscal Year Ending March 31, 1977 (Toronto: Ministry of Government Services, 1978) 18.
- 16 Downsview Computing Centre, Leaside Computing Centre and Queen's Park Computing Centre. For a detailed explanation of the functions and users associated with each centre, see M. Brown, 58-59.
- 17 Ontario, Privacy Project Task Group, Report and Recommendations (Toronto: July 1976) 8-12; Ontario Management Board of Cabinet, Appendix A: Privacy and Security Survey on Information and Individuals (Toronto: Management Consulting Services Division, Ministry of Government Services, August 1975).
- 18 Ontario, Management Board of Cabinet, Confidential Security Audit, 1978. The research staff was not permitted to review the audit report itself, but was permitted to take notes at a meeting discussing its findings.
- 19 However, both the Ministry of Health and the Ministry of Community and Social Services are considering moving towards large, integrated data base systems, which would include data drawn from a number of different programs. This obviously increases the sensitivity of their record systems in that each individual's personal record will contain more information, which will become, in turn, more accessible to ministry personnel.

CHAPTER 27

Personal Information Handling Practices of The Ontario Government

Having established a conceptual framework for the discussion of informational privacy concerns, and reviewed the impact of recent technological developments, we turn our attention to privacy and personal record keeping in the Ontario government. Our mandate directed us to examine two broad issues related to privacy and government information practices:

- the individual's right of access and appeal in relation to the use of government information; and
- the protection of individual privacy and the right of recourse in regard to the use of government records.

Neither of these issues can be adequately investigated without a thorough and current accounting of Ontario government personal information holdings. Accordingly, our initial discussion focuses on the extent and nature of personal records collected by the province. We also review the findings of the studies undertaken since 1968 which provide a historical perspective of privacy and record-keeping concerns in Ontario. Against this background, the findings and conclusions of the Commission's own research on Ontario government record-keeping practices are summarized.

The following account of record-keeping practices in various ministries and programs of the government of Ontario is based entirely on the research work of the Commission's privacy protection study group, and is, in effect, a summary of the case studies reported at greater length in the Commission's research publication, Privacy and Personal Data Protection, by M. Brown, B. Billingsley and R. Shamai.

A. THE EXTENT AND NATURE OF PERSONAL RECORD KEEPING

SOURCES OF INFORMATION ABOUT GOVERNMENT-HELD RECORDS

At present, there exists no complete catalogue or index of the extent and nature of personal records held by the province. Of the following sources, none provides a complete assessment of the number of personal records in government record collections, their location, their contents or their purposes.

Ministry Schedules

In an earlier chapter[1], we described the Records Management Program of the provincial government and the process of "scheduling" records which is its mode of implementation. Each government ministry keeps a schedule of all its records in document or micro-film form in order to control their preservation and destruction. The schedules contain lists of all physical collections including descriptions of each particular group of records and its size. Because the record schedules are compiled by the ministries to control documents and not to provide a compilation of record collections for the purposes of analysis, the Commission was unable to produce from them an accurate or comprehensive listing of record holdings, or to identify which specific records contain personal information.

EDP System Plans

Other sources of information about personal records are the electronic data processing plans submitted by ministries to the Management Board as part of the estimates preparation process. These plans describe all operating and proposed computer systems. The type of record and the data described by these plans would provide a good basis for an index of computerized personal record systems. However, the purpose of the plans is financial control rather than tabulation of computer systems in an easily readable and understandable format.

Catalogue of Statistical Files

Perhaps the best available indication of the extent of personal record keeping by the Ontario government is the Catalogue of Statistical Files which is published by the Ministry of Treasury and Economics. The Catalogue includes a somewhat arbitrary selection of files, many of which contain personal records. Where available, the size of each file is noted. Some important personal record files which would presumably be useful from a statistical standpoint are missing from the catalogue, while others which are included are of dubious statistical value. An attempt is made to indicate the confidentiality of the information, although the categories used do not appear to conform to any standard and are inconsistently applied. In spite of its limitations, the publication provides an interesting overview of the types of data held by the provincial government. However, from the record subject's viewpoint, a list of files used for administrative decision-making purposes, not statistical purposes, would be much more useful.

The Commission's Research Report

According to a recent estimate, approximately 120 automated personal record systems are operated by or are currently under development by the provincial government. Thirty of these were examined for the Commission's research report. Many more manual file systems, which sometimes duplicate what is on computer, are spread across the province in head offices, regional offices, field offices, and private agencies performing contractual work for the government. The number of manual files in the government's charge has never been tabulated; neither has the total number of individual personal records kept by the government.

Wide variations in the size of different record systems make it meaningless to provide numbers or percentages of files or systems containing various types of personal information. To say, for example, that 30 per cent of systems contain sensitive information (more than just name, address, and date of birth) would ignore the fact that some systems may contain millions of records about people, where others contain only thousands, and would therefore give an inaccurate impression. Also, even a name on a certain file (for example, a file of criminal suspects) may be highly sensitive. Nevertheless, we have attempted to describe the size, range and contents of selected records kept by the Ontario government in Table I. Information included in the table was taken from individual interviews, ministry annual reports and the catalogue of statistical files. It should be noted that the degree of detail in the different types of records varies significantly according to the nature and use of the record. For example, "family detail" in most cases is merely a notation of marital status; but in the records of children who are clients of provincial social services, this information may include a detailed description of parental relationships and attitudes.

"WHAT DO THEY HAVE ON ME?"

Anyone interested in finding out what personal information the Canadian government holds about him may consult the federal Index of Information Banks[2] and the department or ministry listed in the index. No similar mechanisms to aid the concerned citizen have been developed by the provincial government. The Commission's report on Privacy and Personal Data Protection provides a somewhat general answer to this frequently asked question:

It depends on who you are -- your age, education, occupation, income and interests. A real estate broker who is married to a teacher, owns property, has a university degree and drives

TABLE I

SIZE AND CONTENT OF
SELECTED ONTARIO GOVERNMENT
PERSONAL RECORD FILES

	Approx. no. of records	Date of birth	Current address	Education	Occupation or employment	Property and assets	Income	Medical	Criminal offences	Family details	Physical description
Vital statistics	8,000,000	X								X	
Licensed drivers	5,000,000	X	X					X	X		X
Vehicles and owners	5,000,000		X			X					
OHIP subscribers	8,000,000	X	X					X		X	
Student health records	600,000	X	X					X		X	
Physicians	14,000	X	X	X						X	
Nurses	90,000	X	X	X	X						
Business registration	40,000	X	X	X	X	X	X		X	X	X
Property registration	n/a	X	X			X					
University students	230,000	X		X						X	
Teachers	212,000	X	X	X	X		X	X	X	X	
Government employees	75,000	X	X	X	X		X	X		X	
Public housing tenants	56,000	X	X			X	X			X	
Welfare recipients	135,000	X	X	X	X	X	X	X	X	X	X
Provincial child wards	13,000	X	X	X				X	X	X	X
Criminal histories (OPP)	400,000	X	X	X	X				X	X	X
Correctional inmates	400,000	X	X	X	X			X	X	X	X

too fast will have more on file about him than someone who is single, works as a store clerk, rents an apartment, has never seen a doctor, and whose main pleasure is watching TV[3].

In an attempt to answer this question more completely, the research group outlined the types of basic records which are collected about everyone in the province from birth to death, as well as those which are collected only from people in certain circumstances or under certain specialized conditions.

The Basic Records

The Ontario government has some information about nearly all of us, which can be readily retrieved by name. If we were born in Ontario the record will have begun with the registration of birth by the Registrar General. During our childhood our schools will have collected substantial information about us (which may be held by the schools, boards of education, or the Ministry of Education/Ministry of Colleges and Universities); through our parents our names will appear in Health Ministry records, and these will contain notations about visits to doctors and major illnesses. In addition, the Health Ministry may have information about us from school health records. When we leave school to start a job or go to university, the number of records begins to multiply. Student loans, taxable income, driver's licences, car ownership and consumer loans all create records about us. These records are all held separately by different agencies of the government.

Specialized Records

These basic kinds of records exist for almost every person in the province. The number and types of other records about a person kept by the Ontario government will depend on the activities he engages in, or the problems he runs into. Many businesses and professions are regulated. Teachers, realtors, car salesmen, projectionists, travel agents, private investigators, and security guards (among others) will all have records kept about them. Everyone who seeks a grant or loan from the government, whether a farmer, a student or a businessman, will have a file opened on him. In most cases such files will contain factual information about financial status, occupation, dependents and education, but some files may also include a physical description and a notation of criminal history, if any. In most situations, this information is provided directly by the individual concerned, although it may be checked against other sources.

Persons in need of assistance from government, or those whose actions government is responsible for controlling, have the most extensive records collected about them. Social assistance, for example, is usually subject to some kind of assessment of need. Therefore, eligibility must be established and monitored. When the law is broken, offenders must be traced and guilt proven. A penalty may be imposed, and will often be determined on the basis of the individual's past behaviour, history and personal circumstances, all of which are contained in considerable detail in criminal records. Information about or obtained from the person's family, friends and employers will be included in such records. In some cases, a psychiatric report may be ordered and retained in the individual's file.

The records discussed above are created in order to regulate people's business activities, to grant a benefit, or to deliver a service. Records may also be created, however, to provide information used by government in planning or research. Census data gathered by the federal government is often shared with the province. Also, some ministries regularly gather their own information. For example, the Ministry of Industry and Tourism collects data about travellers who visit travel information centres; this helps the ministry to determine travel patterns and interests of tourists. The Ministry of Labour gathers data about workers in Ontario from such sources as the Canada Manpower Centre registration forms.

Although these lists and descriptions may help an individual to obtain a basic understanding of what types of information the Ontario government holds about him, they will not assist him in finding that information and determining its accuracy. Nor do these lists enable interested members of the public to evaluate Ontario government information collection practices. Indeed, government officials themselves are not completely aware of the extent and nature of the government's personal record holdings.

B. PREVIOUS STUDIES IN ONTARIO

ONTARIO LAW REFORM COMMISSION

As early as 1968, privacy protection was officially recognized as a growing problem in Ontario. In that year, the Ontario Law Reform Commission published its report[4] which, according to a provincial government task force, "provided the first seminal thinking on the philosophical and constitutional implications of the privacy problem in Canada"[5]. Professor Edward F. Ryan of the University of Western Ontario, who prepared the submission, outlined the areas in which he believed there may be an invasion

of the right to privacy, the extent of such an invasion, current federal and provincial legislation relating to privacy, areas in which the federal government occupied the field of privacy, and areas where he believed the provinces may have the jurisdictional right to legislate concerning privacy protections. In concluding that the effects (if any) of existing legislation on privacy had been secondary and indirect, the submission clarified the need for direct legislation whose primary purpose was the protection of privacy. It was recommended that the province develop comprehensive, unified legislation; the proposals concerning informational privacy included:

- . creation of the offence of invasion of privacy;
- . creation of the tort of invasion of privacy, with appropriate remedies;
- . establishing controls over governmental acquisition, use and disclosure of personal information, with appropriate remedies;
- . defining "consent" in its various contexts where consent means that privacy is not invaded;
- . encouraging the development of organizational and professional ethical standards for the protection of privacy;
- . establishing controls over certain conditions of employment which violate the right to privacy;
- . developing mechanical and electronic safeguards to control unauthorized use of personal information from computer memory banks;
- . specific legislative regulation of the conduct of persons and institutions, the legitimate activities of which per se establish a threat to privacy;
- . establishing rules to create the highest degree of openness for all surveillance by public authorities without unduly hampering the achievement of valid social ends;
- . reviewing and recommending appropriate changes in all provincial legislation in which the considerations of privacy have not been afforded adequate protection.

To "foster the right to privacy in all of its aspects," Professor Ryan saw the need for an independent agency with educational, persuasive, evaluative, investigatory, decisional,

regulatory, reporting and coercive powers, to be overseen by a privacy ombudsman. Finally, it was recommended that a commission or special task force be established to conduct an intensive study of the practical problems involved, and to propose a specific legislative program.

INTERMINISTERIAL COMMITTEE ON PRIVACY

In 1972, in the wake of a far-reaching federal study[6], the Ontario government appointed the Interministerial Committee on Privacy and Computers. The committee examined the implications of the federal report for the province, and attempted to identify provincial privacy concerns, in preparation for a federal-provincial meeting on these subjects. The resulting report[7], although not an empirical study, recognized several privacy and personal record-keeping issues. Several alternative regulatory frameworks were suggested, which would develop norms similar to those embodied in the Ontario Consumer Reporting Act[8], to deal with problem issues such as:

- . third-party access to personal files;
- . the right of a record subject to have access to and to make corrections in personal files about himself;
- . the right of a record subject to participate in decisions made with respect to the use of personal information;
- . the right of a record subject to hold the operator of a file liable for misinformation or false accusations made on the basis of the file;
- . controls over certain types of contents of personal files (for example, arrest records);
- . computer security measures required for files containing personal data;
- . clarification of the status of computer-stored personal data (for example, determination of what happens to personal records when the company holding them declares bankruptcy).

The committee foresaw the possible need for a privacy tort, for an administrative agency created for the purposes of investigations, complaint hearings and encouraging compliance with the law, and for an independent privacy ombudsman[9].

One of the more interesting discussions within the report is an assessment by the Ministry of Government Services of the probable impacts of privacy legislation upon provincial government programs. The discussion assumes that all automated government files containing personal information, including pre-existing ones, would be subject to certain privacy requirements. In particular, all files would be registered with the newly created central Data Protection Agency, which would also serve as an intermediary between file requesters and ministry record holders. Regular file users, such as other ministries, would also be registered with the agency. To implement this organization, the Ministry postulated that all ministries would review and classify all their file holdings, formulate lists of personal record users, tighten security requirements, develop rules for subject access and public access to personal records, and formulate policies regarding record retention. After a brief sample survey of the major holders of files containing personal information in the Ontario government, the Ministry of Government Services concluded that

by careful preplanning, the adverse economic impact of privacy legislation upon existing government programs can be limited or diminished...in general, the arbitrary requirements we have postulated appear to be met, although a more careful examination of this problem may reveal areas of deficiency...it appears that privacy legislation would affect only a small number of the automated files presently existing, and those to a limited extent[10].

PRIVACY PROJECT TASK GROUP

The Interministerial Committee Report was followed in 1975 by a detailed Management Board study[11]. The purpose of the Privacy Project Task Group study was "to identify the Ontario government's level of exposure in the privacy and security aspects of government files containing information on individuals, and to develop appropriate recommendations where necessary." To accomplish this objective, the task group undertook a survey of privacy-sensitive information and associated information-handling environments in nine ministries[12]. The contents, use and security level associated with 107 files containing data were established and analyzed. In addition, a special study of the security procedures and practices in the Queen's Park Computing Centre was conducted. Special attention was given to the identification of current legislation, policies or procedures in the Ontario government designed to deal with some aspect of the privacy/security problem[13].

In appraising its survey results, the task group made the following specific findings:

1. The Ontario government collects an extensive amount of personal information. Although most data collected on individuals is of an uncontentious nature (name, address, etc.), 12 per cent of the 107 systems surveyed collect information on ethnic origin, 11 per cent collect subjective data (opinion), 10 per cent collect data on religion, 6 per cent on race, and 20 per cent on parentage and family relationships.
2. Data on health is common and, while generally treated with discretion, is of particular concern because some medical and hospital data are collected and processed by private-sector agencies, and it is not known under what conditions this information is stored and used.
3. Most files have uses (and thus users) outside the ministry responsible for the data. For example, 8 per cent of the 107 files surveyed are used for the secondary purpose of mailing lists, 21 per cent are used by other governments or police forces, and 16 per cent are used by businesses.
4. Identifiers used as keys for file organization and search purposes are typically selected to serve the purpose for which the file exists, but Social Insurance Number (SIN) codes occur on approximately 50 per cent of files surveyed, providing the possibility of crossover or interlinking of files.
5. There is no consistent policy in the Ontario government covering security of and access to information relating to individuals. The security of personal data depends either upon regulations made under the governing statute (if any) of the ministry or agency concerned, or upon the discretion of the user. It could not be determined how an agency which released data to a third party might enforce its rules of confidentiality or apply penalties.
6. There is extensive dissemination of investigative (criminal) information to other governments, agencies and commissions.
7. Accuracy of personal data is difficult to ensure. Some systems provide for feedback from the subjects as a means of confirmation of the data. In other systems, data may be changed or become obsolete without the subject having any opportunity to confirm its accuracy.
8. The physical security of computer centres is consistent with current accepted standards. However, there are weaknesses in control of areas adjacent to computer facilities, use of temporary personnel to handle personal data, and controls over

access to personal data to computer terminal and computer input/output user areas (that is, areas used for data assembly, preparation, conversion, editing, and distribution). Under these conditions, operating employees with access to the centres would have little difficulty in obtaining data or in damaging data banks and processing equipment.

9. The increasing use of remote terminal facilities for input, output and process initiation means that the security measures used in computing centres will soon protect only computer equipment. The emphasis on security must therefore be changed to user areas to protect against clandestine access to files, programs and other systems software. (The task group was particularly concerned about the security and accuracy implications of placing criminal data on the automated network of the Canadian Police Information Centre (CPIC).)

As a result of its findings, the Privacy Task Group reached these conclusions about the extent of the privacy problem in the Ontario government:

1. There is currently a large and growing potential for invasion of privacy and privacy protection failures in the Ontario government.
2. Current legislation, policies, and procedures dealing with the "right of privacy" and its protection are inadequate, uncoordinated, or nonexistent.
3. The government does not know, on a comprehensive basis and with a reasonable level of accuracy, what sensitive personal information it has, how well it is protected, what it is used for, or the specific statutory authority enabling its collection and use. It does not have a formal conception of the right to information privacy, the rights of Ontario citizens in respect of that privacy, or the obligations of the government to safeguard such rights.
4. The use of information systems embodying data base concepts and sophisticated microrecording techniques is now a practical reality in the Ontario government[14]. With increasing budgetary constraints and the demand for more effective program management and control, there is added incentive for the development of such systems. Without a formal statement of the government's position on the privacy issue, there is a higher probability that these information systems will either exceed what the public is prepared to tolerate in terms of invasion of its privacy or, where an ultracautious approach

is adopted, the optimum opportunities and efficiencies available will not be realized.

To correct what it saw as a growing imbalance between individual privacy and government intrusiveness, the task group recommended broad legislative as well as internal reforms. Because these recommendations are germane to this Commission's own proposals, they are discussed in detail in Chapters 32 and 33 of this report.

C. RESEARCH REPORT CASE STUDIES

In May 1978, our research staff began a detailed study of personal record-keeping practices in the Ontario government, the results of which have been published as a separate document[15]. The purpose of the study, as set out in the staff's terms of reference, was to report on the extent of, and need for, the protection of privacy in personal records maintained by the government of Ontario, and to assess the opportunities for subject and citizen access to personal records. The objective of the study was to determine whether generalized regulations and legislation governing privacy of personal records would be appropriate, and to suggest policies for each type of personal record considered.

The most significant part of the study was concerned with gaining a detailed understanding of how certain types of records about people are gathered, maintained and disseminated by Ontario government ministries and agencies in each of six specific areas: Education, Health, Social Services, Corrections, Law Enforcement and Government Personnel. Because the Royal Commission of Inquiry into the Confidentiality of Health Records, chaired by Mr. Justice Horace Krever, was in the process of completing an investigation of record keeping in the health field, the major issues in that area were simply summarized to avoid duplicate research efforts and will not be referred to here. Additionally, less detailed case studies were conducted of three personal record systems frequently seen as controversial by members of the public: the Personal Property Security Registration system (PPSR) of the Ministry of Consumer and Commercial Relations, and the Licensed Drivers System and Vehicles Registration System of the Ministry of Transportation and Communications. A summary of the record systems examined is contained in Table II.

The group also investigated two general privacy and record-keeping issues which concern the entire Ontario government: expanding use of single identifying numbers (discussed in Chapter 28) and rapidly developing computer technology (discussed in Chapter 26).

TABLE II

RECORD SYSTEMS EXAMINED
BY THE PRIVACY STUDY GROUP

Social Services

Adults:

Family benefits
General welfare assistance
Vocational rehabilitation
Mental retardation

Government Personnel

Pre-employment records
Ministry personnel records
Integrated pay, personal &
employee benefits
Security clearance records

Children:

Children's aid societies
Adoptions
Child abuse register
Training schools
Juvenile probation
Day nurseries

Law Enforcement

Canadian Police Information Centre
Criminal history
Criminal occurrence
Identification
Intelligence

Health:

Senior citizens' drug
benefits

Corrections

Adult inmates
Probation and parole

Education

Student awards
Pupil records
Teachers certification
Trade certification

Others

Licensed drivers
Registered vehicles
Personal property security
registration

The study group undertook the major part of its investigative work during the months of May, June, July and August 1978. To obtain a practical appreciation of privacy concerns in each area, extensive interviews were conducted with administrators and operating staff at all levels of government, and on-site inspections of both manual and automated information processing environments were made. Relevant outside agencies and organizations provided another perspective.

EDUCATION

Elementary and Secondary Schools: Student and Teacher Records

The major types of student records kept at the elementary and secondary levels are the Ontario Student Record (OSR), guidance reports, student health records, psychological reports and attendance records.

Ontario Student Record (OSR)

The Ontario Student Record (OSR), defined by the Pupil Record Regulation[16], contains information respecting a student's progress and achievement in school, and includes parent and teacher comments. In 1974, section 231 of The Education Act[17] was amended to allow parental or pupil access to the OSR. This section created a mechanism for correcting the record, more closely defined the record's purpose, limited third-party access to the record and restricted its use for evidential purposes. Because section 231 was the first major provincial statute to fully protect the subject of personal data collected by a public authority, the Commission closely examined its implications for educational record keeping.

One of the first results of section 231 was a completely changed OSR form, redesigned to more specifically meet the statute's purpose and to eliminate negative subjective data which might be harmful to the subject. Teachers interviewed about the changes in the law and the OSR form have said that they no longer feel free to record impressionistic observations about their pupils, and that the OSR is therefore no longer as useful in alerting new teachers to students' problems. As a consequence, opinion information is now more frequently communicated orally in an informal fashion. The teachers continue to make their reports briefer and more objective, despite statutory immunity from civil actions respecting information in the record.

Many school authorities feared that the projected large volume of inquiries regarding the OSR would cause problems. In fact, few access requests have been received since section 231 came into force. However, a constant flow of complaints from parents worried about possible adverse information in pupil records ceased after passage of the law. The research report concludes

While the provision has not been widely utilized, there is some indication that it has responded to a publicly perceived need. The availability of files seems to reassure the public, without taking further action, of the propriety of record keeping[18].

However, in the course of the research, other privacy issues emerged, such as the inaccessibility of certain types of records which, although not part of a student's official record, contain judgments sometimes used in decision making; the propriety of collecting certain sensitive data (for example, psychological data) in the schools and the problems of maintaining such data in a confidential manner; the ambiguous status of school health records and health record-keeping personnel, and the potential uses of the school attendance record for far-reaching non-educational decisions about pupils.

Teacher Records

Official teacher records, including proof of certification, are held by the Ministry of Education in its information systems and records branch. Evaluation reports about the performance of individual teachers are kept by local boards who employ them in what are known as "correspondence files." Decisions concerning a teacher's career may be made on the basis of materials in both of these types of files. Although some collective agreements in the province include a provision for subject access, no uniform access policy for teachers in relation to their employment records has been implemented. In the absence of consistent guidelines, inequities in the access process have developed, resulting in different treatment of similar requests.

Colleges and Universities: Industrial Training, Trade Certification and Student Awards

The Ministry of Colleges and Universities is responsible for administering capital and operating grants to universities and colleges, financial assistance to students, and certain programs relating to trade certification and training.

Industrial Training and Trade Certification

The ministry keeps records of industrial training course enrollees in order to verify that certain ministry-set requirements for certification are met, and to account for student tuition and living allowance expenditures paid by Canada Manpower. In the course of training, apprenticeship, examination, qualification and the continuing regulation of trades, a great deal of information concerning both the training program and the individual is collected. The records determine not only whether a student succeeds or fails in the particular course, but also affect his training allowance from Manpower, the rate of apprentice wage set by the regulated trades, and ultimately the rate of pay commanded by a qualified tradesman.

The industrial training student, unlike the elementary or secondary student, has no rights of access or correction to the one record which obviously has a tremendous bearing upon both continued employment in the program and future employment in industry. Nor is the use and transfer of the record by college authorities subject to his consent.

Student Awards

The student awards program is administered by the Ministry of Education and Colleges and Universities for the purpose of distributing funds on a grant or loan basis, to post-secondary students at Ontario universities and community colleges. The program currently consists of several plans: the Ontario study grant plan, the Canada student loans plan, the Ontario student loans plan, and the Ontario special bursary plan at the undergraduate level, as well as Ontario graduate fellowships, bursaries for second language teachers and fellowships for second language study. Eligibility is determined based on work and study history, marital status, residency and citizenship, the duration and nature of the education program and the income available to the student.

Since 1978 applicants have also been required to give approval for release of tax information and a statement of assets. Tax returns were previously used by student awards officers to verify income, but only in a sample of cases selected after the awards process. Now, all applying students must authorize release of their entire tax returns, despite the fact that the ministry uses only the income amounts stated on the returns to verify the income amounts on the student award applications. If there is a discrepancy, additional information may be taken from the student's return. Although applicants are made aware that verification will

occur, many are upset by the intrusiveness of the mandatory transfer of a document which has traditionally been considered both confidential and to be used for one purpose only. Moreover, applicants are not notified of the nature of the verification process or of the confidentiality safeguards for tax information.

The statement of assets has received similar criticism. It contains personal information not normally found on any other record, such as details about the student's (and parent's or spouse's) real estate investments, personal property and business holdings. No indication is given as to the extent to which that information may be seen or used by persons outside the student awards administration.

GOVERNMENT PERSONNEL

The Ontario government employs office clerks, highway engineers, lawyers, chemists, police officers, computer experts, economists, drivers, doctors, teachers and many other categories of workers, and like any large employer, it keeps a variety of records relating to its employees. This section examines the personal information practices of the government in its role as employer by focusing on the collection, storage, maintenance, and transfer of information about its employees. The issues of subject access and correction rights are also discussed.

The amount of information collected by the government as employer has been reduced by changes in the standard employment forms for the civil service in the interests of applicant privacy protection. For example, applicants are no longer asked for weight and height, maiden name or whether they have use of a car. Less health-related information is requested, and in general, the purpose of the information elicited on the form is now indicated. Some changes in the new form eliminate references to what were, in fact, infrequently performed verification processes. These changes reflect a sensitive appreciation of privacy protection principles.

The nature and amount of information required depends on the type of job being applied for. For example, applicants for positions in the Lieutenant Governor's office, the Premier's office and various branches of the Ministry of the Solicitor General are subject to security checks undertaken by the security branch of the Ontario Provincial Police. Criminal records checks on applicants are also undertaken for a variety of sensitive positions within other ministries. While this may be a necessary precaution, one aspect of this practice raises a concern for the privacy of candidates: subjects who are denied clearance are not given access to the investigative file nor reasons for the denial.

All personal information about government employees is held in a variety of computerized and manual files kept by several different authorities over the course of an employee's career. In 1976, employee information for payroll, personnel, and benefits administration purposes was merged into the Integrated Pay, Personnel and Employee Benefits System (IPPEBS). The IPPEBS data base is used for payroll preparation and to generate and update an employee service record report. This single document contains information about individual classifications, transfers from job to job, salaries, benefits, income tax exemptions, social insurance number, sick days, and vacations.

The purpose of the merger was to reduce the duplication of information common to all three files and to increase efficiency and completeness of the record-keeping process. It allows the Civil Service Commission (CSC) to adjust personnel inventory, budget for projects, and perform other statistical manipulations with greater ease. Moreover, the overall staff is expected to decrease as a result of the combining of these systems. In ministries which had previously required personnel clerks, payroll clerks and employee benefits clerks, IPPEBS clerks now fulfill all three functions.

The implementation of the IPPEBS provides an interesting illustration of the privacy implications which can arise from increased efficiency of data systems. For example, the Civil Service Commission has developed a plan to include subjective material found in letters of reference and detailed work and education histories in the computerized data base. This information would constitute a valuable "skills inventory" for use in personnel planning. On the other hand, the computerization of such sensitive data does raise concerns about individual privacy because of the increased potential for access and abuse. A second illustration relates to third-party access to personal files. At present, few ministries have formulated any written policy on this question, and in practice personnel branch staff have virtually unlimited access to such files. Because of this potentially privacy-invasive factor, at least one ministry has refused to amalgamate all record-handling duties, and has separated clerical payroll and benefit operations from personnel matters. At present, record subjects are not made aware of what information is automated and what remains in manual form, nor are they given the opportunity to check the accuracy of computerized information.

In addition to the computerized files, there are a number of types of manually-held employee files. Certain manual record-keeping practices also raise privacy concerns. For example, repeated absenteeism or inability to perform adequately may cause an employee to be referred for medical assessment during his

employment. A "mandatory referral" may be made where alcohol or drug abuse is suspected. The authority for such examination is found in The Public Service Act[19] or the collective agreement respecting employee benefits, for employees covered by that agreement[20]. Originally, the purpose of the mandatory medical assessment was to ensure that sick pay provisions were not abused, but it is now also being used as part of the government's alcoholism treatment program[21].

Record keeping for the mandatory referral program poses two privacy problems. First, although the "authorization and release" form appears to request employee consent for release of records about his diagnosis and condition to the referring ministry supervisor, an employee whose examination is duly required and who wishes to remain employed has no choice but to sign the consent. A refusal to sign the authorization is considered a refusal to have the medical examination, which may be considered grounds for dismissal.

Second, records of sensitive personal information generated by the government's alcoholism treatment program are not granted the same confidential status as other medical records generated in the course of the employer-employee relationship. If a ministry official initiates a referral to the program, a warning letter is sent to the employee stating that his performance problem is perceived by the employer to be rooted in alcohol use. A copy of the letter stays in the employee's basic personnel file. After the medical examination, a report on the prospects of improved performance, diagnosis, and treatment program outline are sent back to the personnel department and also placed in the file. Thus, sensitive medical information is stored together with the more routine documentation in the personnel file with the consequent possibility of access by supervisors and co-workers.

Employees have an obvious interest in examining information about themselves which may be used in decision-making processes, in order to ensure that it is fair and accurate. However, the government of Ontario has no uniform policy governing an employee's access to his own records. Government departments and agencies follow a wide range of practices regarding subject access and correction. At present, there are also variations among collective agreements governing union access to personal files for grievance purposes. In some cases, access to a file may not be granted until the dispute goes to the Grievance Board.

Policies on third-party access to personnel files also vary by ministry. The ministries of Industry and Tourism, Housing, Natural Resources, Environment, Education, Solicitor General, and Correctional Services are the only ministries which have formulated written rules concerning third-party access to personnel

files. Development of policy in this area is particularly important because of the variety of requests for information in personnel files which occur from within each ministry, from one ministry to another, and from members of the public. In some ministries, at least, it appears that police are given access to government personnel files on request. Unrestricted police access to personal information in the absence of a subpoena or search warrant constitutes a potentially serious threat to the individual privacy of record subjects.

In summary, then, although the Ontario government as an employer has attempted to reduce the amount of information it collects from job applicants in the interests of their privacy, it has not developed an overall policy in areas such as subject access and transfer of personal information about its employees to ensure that individual privacy is protected in other employment situations.

SOCIAL SERVICES

The volume of personally identifiable records held by social service agencies in Ontario is large and growing larger. The Ontario Ministry of Community and Social Services, which administers the majority of social service programs, and its contracted agencies now hold the personal records of over 230,000 adults[22] and at least 300,000 children in the province.

The types of information collected about those who come into contact with social service organizations is of a personal and sensitive nature. The collection of this kind of information is inherent in social service programs; the social service professions have traditionally used personal information about their clients to diagnose problems and to design treatment plans. As a result, their records often contain details about clients' physical and mental health, education, personal and family history, contacts with the justice system, finances, sexual activities and living circumstances. Recording of these details is facilitated by large "narrative" and "comments" sections on record forms[23].

Several statutes give broad information collection powers to public social service agencies. For example, the statute which requires unmarried deserted mothers who receive public assistance to make efforts to obtain support for their children can only be enforced by requiring that applicants identify and, if possible, locate the father. In some cases, this may mean revealing details about the history of the relationship.

Such requirements may invade the privacy of the applicant. Although a great deal of the personal information collected by

social services is required by statute, in other cases interviewees reported to our researchers that some data items not expressly required by statute were collected simply because this has always been done in the past.

Methods of verification of information supplied by applicants for public assistance are often contentious. For example, they may be required to produce bank statements, insurance policies, birth certificates of all dependents, documentation of marriage and divorce, rent and utility receipts, letters from employers, school attendance records of all children over sixteen years old, and evidence of indebtedness. Often this information can only be supplied with the cooperation of third parties, who then become privy to the fact that a person is applying for public assistance. From the applicant's point of view, an even more contentious practice is the occasional recourse to neighbours, acquaintances and home inspections in order to verify information supplied.

The privacy implications of social service legislation are rarely the subject of public debate before legislation is enacted. As yet, no official extra-ministerial body has been charged with the responsibility of reviewing proposed legislation to assess its impact on individual privacy. The Children's Services Division Task Force on Legislative Amendments has set an example in this area by considering the importance of privacy in its recommendations for changes in statutes governing children's services[24].

Our researchers found that the absence of an overall policy to ensure that records containing personal information are secure has led to inconsistent practices among different programs, agencies and individuals, many of which do not provide adequate protection for the privacy of applicants. Nor does the ministry regularly destroy or de-identify the personal records of unaccepted applicants, persons who are no longer recipients or juveniles who have reached the age of majority. The retention of records of juvenile former clients and of those transferred to adult services at the age of eighteen creates the potential for unauthorized dissemination of possibly detrimental information about juveniles to the public and to adult authorities. Some officials interviewed by our research staff estimated that the destruction of inactive or outdated records would reduce the present volume of personal social service records in Ontario by over 150,000 individual files making the data security responsibilities of the ministry more manageable.

The increasing use of computerized information systems in the social services field, as elsewhere, gives rise to privacy-related concerns. The transfer of data items, particularly those of a subjective or speculative nature, from manual records to computers may result in incompleteness or distortion of information.

Computerized information systems rarely allow for qualifications or explanations of data items. As a result, data subjects may be permanently "labelled" in an unfair or misleading manner. The privacy implications of this issue become more serious in view of the trend toward the integration of social service computer systems in Ontario.

Integration among similar-function programs, such as income maintenance programs, might actually reinforce applicant privacy by eliminating record-keeping duplication. However, the integration of public assistance data banks with those of housing programs, health systems, programs for the disabled, and day care information systems which has recently been proposed raises certain privacy issues. Integration of different-function data banks increases the possibility of unauthorized access to personal data, which further diminishes privacy.

At present, there are no legal sanctions for violating privacy or disregarding record confidentiality. Although many verbal reprimands have been issued when personal information has been revealed, written reprimands, loss of pay or dismissals have been rare, even for serious violations of confidentiality.

A further problem in this area is that social services employees are not given adequate training with respect to the privacy of applicants and clients and the need to safeguard the confidentiality of personal records. Our researchers found that most of those interviewed had been given no instruction in data protection responsibilities during their formal training. Training personnel in several social service programs acknowledged the lack of direction in this area.

The Ministry of Community and Social Services is currently in the process of developing policies and guidelines to deal with these issues. A policy statement adopted by the Ministry in October 1979, sets out a statement of general principles with respect to confidentiality and release of information and requires that each program area develop written policies in accordance with these principles for their particular services. Written policies are to be drawn up with respect to the justification for the type, nature and degree of data collection, the security of records and their retention or destruction, and the conditions under which personal information will be made accessible to third parties and to record subjects. In addition, the policy statement recommends that an administrative appeal procedure be developed internally to deal with disputes over subject access to records. Any employee violations of the policies and procedures developed will be subject to internal disciplinary sanctions.

This new policy would allow record subjects to examine the factual information which they have provided, for the purposes of checking the accuracy of their files. In addition, access may be permitted to information in the file provided by other parties about the record subject if it could potentially affect his status.

As for the release of information to third parties, the policy statement provides that information may be provided, without the client's consent, to the coroner's office, the Ombudsman, the courts on court order, other officials who have authority under provincial or federal statutes to examine the files, the minister and officials to whom he has delegated the authority, and government officials within the same division of the ministry who have been designated by the division. In any other case, access by third parties can only be given with the informed written consent of the record subject. Record subjects must be notified of any release of information. In a case where a consent is refused, the minister may authorize the release of information if he deems it to be in the public interest. A list of all releases made in these circumstances will be tabled annually in the legislature.

Privacy issues in the Children's Services Division of the ministry have been the subject of ongoing review and analysis by the Task Force on Case Information Disclosure since 1977. The Task Force has engaged in an intensive study of various issues in this area with a view to developing new policies and procedures to protect the privacy of children. The final report of the Task Force with its recommendations was released in 1979 for public discussion[25]. In addition to the work of the Task Force, other personnel within this division have formulated, in consultation with other social service agencies and members of the public, privacy standards for information systems and residential services[26]. Our research staff found the initiatives in this area to be very encouraging.

LAW ENFORCEMENT

The gathering and handling of personal information by law enforcement agencies raises particularly difficult issues of privacy protection. It is inherent in the nature of law enforcement activity that highly sensitive personal information will be gathered for the purpose of making law enforcement decisions relating to the data subject. Data will be gathered without the knowledge or consent of the data subject by methods which would, by any reasonable standard, be considered to be invasive of personal privacy. Public tolerance of these invasive practices is premised, of course, on the need for effective law enforcement as

a means of preserving public order. On the other hand, it is widely accepted that there are limits to the extent to which the public interest in privacy protection should be sacrificed to the public interest in effective law enforcement.

Organization of Policing in Ontario

Policing in the province of Ontario is carried out by three police forces. Generally speaking, the members of the Ontario Provincial Police (OPP) exercise powers and perform duties in the preservation of the peace and suppression of crime in the province. There are 180 OPP detachments around the province, with the force's headquarters in Toronto. Also, there are 128 municipal police forces, ranging in size from 5,300 uniformed officers in metropolitan Toronto to a single officer in some small towns. The Royal Canadian Mounted Police (RCMP) are concerned with certain specialized aspects of law enforcement (such as drugs, or inter-provincial transport of stolen goods) in the province in cooperation with other forces.

In the Ontario government, responsibility for law enforcement rests with the Solicitor General, who administers the Police Act[27]. Through the Solicitor General, members of police governing authorities are appointed. The Ontario Police Commission monitors policing standards in the province and is responsible to the Solicitor General. The commission also provides training to police forces at the Ontario Police College, as well as technical advice. It is not uncommon for investigations to be carried out through the joint efforts of several police forces. Police at the federal, provincial and municipal levels may retain overlapping or duplicate records on an individual or incident.

The Sources of Law Enforcement Information

It is useful to distinguish between two major types of law enforcement information-gathering activity: the investigation of specific occurrences, and the gathering of "intelligence." Two aspects of intelligence may be considered in turn: intelligence concerning crime, where ongoing efforts are devoted to the detection and prosecution of crime, and security operations, which are designed to identify and prevent the realization of threats to the government and to the political stability of the province. This latter category includes subversive activity and threats to the lives of important public officials. "Occurrence investigation" refers to a specific incident, while intelligence gathering is concerned with a pattern of occurrences, or with the prevention of occurrences.

Certain types of personal information are also generated through the process of law enforcement, such as records of arrest, prosecution, disposition and sentence. Documentation relating to search warrants and wiretap authorizations (even where they are not granted), and transcripts of trials, appeals and related proceedings contain personal information generated by the law enforcement process.

The potential sources of investigation information and intelligence are virtually unlimited, but an important source is individuals who voluntarily supply information to the police. According to the police, other sources of personal information (apart from individuals) used by police are public and private institutions such as government ministries and agencies, banks, hospitals, telephone companies, credit companies, and other law enforcement agencies[28]. Police may gain access to information which would not normally be public without a search warrant or other judicial authorization if the institution in question is willing to provide it voluntarily.

Without a more detailed inquiry, it is not possible to assess the extent to which these institutional sources of information are used by the police. However, as we describe later in this chapter, Ontario police officials have direct computer access to the vehicle and driver licensing files maintained by the Ministry of Transportation and Communications. Access by law enforcement authorities to medical records maintained by both public and private institutions is currently undergoing study by the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario.

Computerized Records Held by Police

Ontario police forces have for some time been using computerized information systems both locally and in connection with larger networks[29]. Two computerized systems are now in use on a national basis in Canada: the Canadian Police Information Centre (CPIC) and the Automated Criminal Intelligence System (ACIS). CPIC is a large computerized information bank operated by the RCMP, which serves as an index to information held by local or provincial police forces throughout Canada[30]. CPIC holds information arising out of day-to-day police operations such as information about wanted or missing persons, persons prohibited from driving motor vehicles, stolen property and firearms. Also, the RCMP makes available through CPIC individual criminal record synopses which serve as an index to the full criminal records held by the RCMP.

All Ontario police forces that provide 24-hour round-the-clock service are linked to the CPIC computer through a communications network and approximately 250 remote terminals in police stations and patrol cars. The network is also used for teletype communications between individual police forces. All CPIC information (except the criminal record index) originates with a police agency, which is responsible for updating, correcting or removing the information it has placed on the system. No police force may alter information provided by another force. When requested information is transmitted from CPIC, the message concludes with a suggestion that direct contact be made with the force holding the original data. By checking the detail and accuracy of the CPIC information with the original supplier, an attempt is made to ensure that action is not taken on the basis of erroneous data. On the basis of a CPIC message, police may, however, hold a person suspected of being wanted on an outstanding warrant until confirmation of the data is obtained from the originating police force. CPIC is thus an important and increasingly powerful tool for operational law enforcement.

The second major computerized national police file is the Automated Criminal Intelligence Service (ACIS), which is a computerized intelligence communications network administered by the Criminal Intelligence Service for Canada (CISC), the coordinating body for nine provincial intelligence bureaus. The information placed on the system is retrievable by means of various personal identifiers, the individual's physical description, and the geographical location or crime category. An entry may contain any of forty-eight different types of descriptive data, including the subject's criminal history.

ACIS contains reports contributed by twenty-eight member and eight affiliated bureaus. In Ontario, the Criminal Intelligence Service for Ontario (CISO) collates and distributes information supplied by its members. CISO is an association of intelligence officers from the major urban police forces in Ontario, the OPP and the RCMP. CISO members are the only Ontario police authorities who have access to information held by ACIS. However, information obtained by a CISO member may be disclosed, at the member's discretion, to an ordinary investigating officer for use in a specific investigation.

The ACIS network is directly linked to CPIC. When an inquiry is made to CPIC about a person who is also listed in ACIS, the ACIS operator receives a signal to indicate this. The ACIS operator may ask the investigating officer for further information on the location of the listed individual. (ACIS is "blind" to the CPIC system in that the officer who queries CPIC would only learn that the subject of his inquiry is on ACIS files if the ACIS operator relays this information to him.)

In a large country such as Canada, coordination of law enforcement information would be difficult or impossible if computerized networks were not available. The development of the ACIS system has substantially increased the capacity of those agencies and individuals engaged in intelligence work to effectively share and use intelligence information, and the speed with which this kind of information can be retrieved has been dramatically increased through the use of computers. The ACIS system assists the police in surveillance of any individual whose activities involve numerous locations. Further, the ability to use intelligence information from a broad range of sources in analyses of the activities of a particular individual or group may be especially useful in efforts to monitor and curtail the activities of organized crime.

However, as we have indicated in Chapter 26 of this report, there are a number of privacy protection problems inherent in the use of computers. For example, the need to convert detailed information (sometimes based on opinion rather than fact) to coded computer language may reduce its accuracy. A recent study of computerized criminal justice records in New York State indicated that only 27 per cent of the files were accurate and complete[31].

The computerization of law enforcement systems is a subject which has given rise to considerable uneasiness in other jurisdictions. In considering this issue, the recent report on the British Data Protection Committee made the following comments:

We think it is most important, if the confidence and respect which, by and large, the public in our free society still has for the police is to be preserved, that major policy decisions about computerized policy applications handling personal information should not be taken in secret[32].

It is obviously rather late to offer similar advice with respect to the implementation of such systems in Ontario. However, it should be noted that there appears to be no formal mechanism in place even now to ensure that public discussion will precede the implementation of any proposals to alter or extend such networks, to link them to other existing systems or to establish new information systems in the future.

With respect to the scope of intelligence record keeping in general, it is important to remember that the subjects of such surveillance may be individuals who have never been convicted, or indeed accused, of any criminal act. Moreover, the names of persons who have merely had innocent contact with subjects of surveillance may appear in intelligence files and in the computerized name file. The broad range of potential sources of such

information and the unverifiable nature of some of the information which may find its way into the system gives rise to classic informational privacy problems and suggests that the scope of such surveillance should be carefully limited to cases where a clear need for it can be demonstrated.

These concerns are especially serious with respect to the gathering of political intelligence. Difficult lines must be drawn between surveillance of individuals who are prone to committing acts of political violence and subversion, and those who pose no threat and are merely exercising democratic rights of dissent. It is important that these distinctions be carefully drawn in such a fashion that the public will have confidence that proper limitations on surveillance activity are being observed by the security services.

At present, no clear statutory standard governs the scope of intelligence record-keeping activity in Ontario, nor has a power of inspection and comment regarding this activity been bestowed on any independent body or official. Some jurisdictions have adopted such standards in legislation[33]. The state of New South Wales, Australia, has given its Privacy Committee broad powers to examine and report on law enforcement intelligence files[34]. In Sweden[35] and France[36], similar powers have been bestowed on a public official. The British Data Protection Committee also recommended that police intelligence systems should come under the supervision of its proposed Data Protection Authority[37].

Disclosure of Law Enforcement Information to Third Parties

A question of obvious relevance to the privacy protection issue is the extent to which access to law enforcement information is granted beyond the confines of the law enforcement community. Of particular interest is the extent to which criminal record information is made available, on request, to individuals or institutions who may have an interest in such material. In theory, criminal record information is part of the public record in the sense that it is contained in the records generated by the court system in its disposition of criminal prosecutions. However, for all practical purposes it is inaccessible to the general public because court records are not centrally collated or stored. Thus, the advent of the centralized criminal record system through CPIC operated by the RCMP creates an information resource (albeit one consisting largely of information which has never been "secret" as a matter of law or policy in the past) which is capable of permitting new and possibly privacy-invasive uses of criminal record information by making it more accessible.

The OPP forwards requests for criminal record checks to the RCMP only in response to requests from Ontario government agencies which have been approved by the commissioner of the OPP[38]. Most of these agencies have a statutory basis for seeking such information as part of a licensing scheme which explicitly makes "past conduct" a relevant criterion to be considered in deciding whether to grant the licence in question. In response to criminal record inquiries of this type, the OPP releases only conviction data to the government agency.

As far as local police forces are concerned, a survey of ten municipal police forces indicates that policies governing access to criminal records vary from one force to the next. Some forces provide such information only to other police forces. Others also provide information to Children's Aid Societies, Big Brothers, and local licensing authorities as well as agencies such as the John Howard Society. One force indicated that it would provide information to employers with respect to a job application, but only if the applicant was aware that such a check would be made. The nature of the information provided also varies considerably. Some forces provide a complete record of convictions. Others advise whether a record is "serious" or "not serious."

Although policies vary considerably, the authorized release of criminal record information to non-police agencies appears to be limited. However, incidents reported in the press suggest that criminal record information may be passed on to private companies in contravention of policy, particularly in situations where, for example, a private investigator who is an ex-police officer has maintained contact with former colleagues[39].

Another point concerning third-party access to law enforcement information must be considered. The third party requester normally seeks access for the purpose of making a decision of some kind relating to the data subject. It is thus important that the data subject have the opportunity to ensure that the information which the third party receives is accurate. Since criminal records are available to the data subject from the RCMP, there should be no objection to allowing him to ensure the information transferred to a third party is accurate. Security checks, however, raise more difficult issues because they often contain information which law enforcement officials would not want disclosed to the data subject for fear of compromising confidential sources or investigative techniques. As we noted earlier, because data subjects are not told the substance of allegations in "negative" security checks, they cannot question their accuracy. It is possible, then, that a data subject may be deprived of an important job opportunity on the basis of information whose accuracy he cannot verify.

Subject Access to Law Enforcement Information

Subject access to files containing personal information is one of the principal mechanisms for ensuring that fair information practices are adopted by agencies which gather and use such information. Without doubt, law enforcement information systems provide the most difficult context in which to implement this principle. Obviously, there is a very compelling interest, as far as the individual is concerned, in learning as much as possible about the contents of law enforcement information systems which concern him. On the other hand, there are undeniably compelling interests in secrecy in order to facilitate effective law enforcement activity. As we indicate elsewhere in this report[40], other jurisdictions have attempted, in freedom of information and privacy legislation, to draft exemptions from the general principle of subject access which would protect the need for secrecy with respect to such matters as the identity of informants, law enforcement techniques, and information contained in files related to active investigations, while assuring citizens that any personal information falling outside this range of protected interests is accessible. In Ontario, law enforcement agencies are at present under no legal obligation to give data subjects access to files containing information about them.

CORRECTIONS, PROBATION AND PAROLE

The Ministry of Correctional Services is responsible for administering all adult provincial correctional institutions and jails as well as provincial adult probation and parole programs. In general, the ministry deals with offenders sentenced to terms of less than two years, although those sentenced to longer terms and therefore destined for federal institutions also pass through the ministry's hands at some point.

The ministry also supervises persons on parole from provincial institutions and on probation. Parole is a means of releasing an offender into the community under supervision while he serves the remaining portion of his sentence. There are parole boards at both the federal and provincial levels, but the Ontario Board of Parole makes parole decisions for all inmates in provincial institutions[41]. Probation is where the court imposes a sentence with permission to serve it at liberty in the community subject to conditions prescribed in the probation order.

Although large numbers of people are dealt with by the ministry[42], the majority of them are held for only short periods pending payment of a fine, release on bail, or the serving of a brief term of incarceration. In such cases, personal information

collected by the ministry is generally limited to biographical details. However, when a person serves a longer sentence, the information collected may include psychiatric assessments and routine reports on his behaviour and attitude. Similarly, a person who is placed on probation or parole is subject to supervision by an officer of the parole board and is subject to be reported on in detail. Thus privacy issues arise in connection with different records held by the Ministry of Correctional Services.

It is apparent from our research that the ministry regards the confidentiality of information retained on the people with which it deals as a serious matter. Files on inmates are closely guarded. In the correctional institution visited by our research group, files were kept in one central location to which access was restricted. In addition, the ministry has developed an extensive policy on confidentiality, which might serve as an example to other ministries and to the government in general. The policy directs how written and telephone inquiries should be handled, whether the inquirers are police, courts, lawyers, news media or others and central records section staff are trained in implementing the policy. All employees must also follow the requirements of the confidentiality section of the new Ministry of Correctional Services Act[43]. No penalties, however, are attached to the contravention of this section.

While the sharing of information from an inmate's or probationer's file with third parties is closely controlled under current policy, questions concerning subject access to personal information have yet to be discussed. The person who has the greatest interest in ensuring accuracy of information, and who must be protected from the impact of an erroneous record, is the inmate or probationer. On the basis of information collected about an inmate, decisions are made about the kind of institution he is to be assigned to, any special treatment he is to receive, and whether he will be granted a temporary absence permit. Although he may be aware of much of the information leading to these decisions, the inmate is not normally permitted to see the actual file. He likely will have already seen the pre-sentence report and the warrant of committal and may receive or be shown copies of misconduct reports and temporary absence applications. He may not, however, see the inmate record card (which may indicate, for example, that the inmate is assaultive, a sexual deviate, or an arsonist) nor generally know the contents of the progress reports or psychiatric assessments. Some correctional staff members pointed out that a notation on a file may cease to be applicable but may remain on the file unless it is specifically removed by a member of staff who decides that it is incorrect. In addition, when files from previous sentences are referred to, information which is out of date could influence a decision about

an inmate. Our research staff found that the inmate files they examined at random did contain many subjective observations. However, reports by probation officers, including pre-sentence reports, have apparently improved in quality and objectivity as a result of better training and greater openness. In the probation files examined, reports by probation officers appeared to be more factual and more objective than psychiatric reports. A 1976 study of the parole process by the Law Reform Commission commented on the need for clarity, consistency and uniformity in reports about inmates and parolees[44]. While objectivity of reporting might improve further if subject access were permitted, it is possible that subject access would result in loss of some useful subjective data. In re-examining the merits and dangers of including such information in personal files, the ministry is trying to strike a balance between the need for information and individual privacy.

In parole reports, family members and friends are often asked for their frank opinions about the impact of an inmate's release on the community. Some ministry officials believe that inmates having access to such reports may retaliate against those who expressed negative opinions. Moreover, traditional sources of information may refuse to cooperate with authorities if they fear record subjects may identify them. If a subject access policy is implemented, care must be taken to mask the identities of sensitive information sources.

A projected large volume of requests to review files, and the resulting increase in paper work and costs, is also seen as a drawback to a subject access scheme in the Ministry. The experience of the Canadian Penitentiary Service with a subject access scheme since the implementation of the Canadian Human Rights Act indicates that inmates do use such a scheme more frequently than other record subjects. However, the number of applications to the penitentiary service substantially decreased after the first year. More important, the large volume of requests influenced the service to reform many of its record-keeping practices and amalgamate several of its files, thus reducing the time needed to review information for subject access purposes.

PERSONAL PROPERTY SECURITY REGISTRATION SYSTEM

Some personal record-keeping systems maintained by the provincial government are established for the purpose of creating public registers. One example of an Ontario government-held collection which is open to the public is the Personal Property Security Registration (PPSR) system, administered by the Ministry of Consumer and Commercial Relations.

The system, implemented in April 1976, amalgamated and automated a number of separate county- and district-held manual files used in the registering of personal property as security against loans under The Personal Property Security Act[45]. According to government officials, the amount of information required for the new system was reduced from that required for the former manual system because of questions relating to data confidentiality and privacy. The act, and hence the system, applies to every transaction that creates a security interest, including a chattel mortgage, conditional sale, equipment trust, floating charge, pledge, trust deed or trust receipt, and an assignment, lease or consignment intended as security. Both individual and corporate debtors are included on the file. The credit grantor provides a completed registration form from which all information is taken and recorded on a computer file. The minimum amount of information required to register a security is the name and address of the debtor, the secured party (the creditor) and the collateral classification[46]. Although the principal amount secured must only be stated with respect to security provided by individuals in a consumer transaction, in practice the principal amount is often included on business files as well.

The Ministry of Consumer and Commercial Relations operates the PPSR system on a cost-recovery basis. A schedule of fees for registration and inquiries has been established. Daily tapes are sent to the Associated Credit Bureaus of Canada, which distribute information from the tapes to their members. This service is carried out on a contract basis for a fee which recovers the cost of tape processing and transmission. The ministry also contracts with Dun and Bradstreet to provide daily information on business debtors and securities from the system. Debtors are not informed that PPSR information will be sold to these credit reporting agencies.

Two searches may be made of the individual debtor file. If the requester knows the surname, given name, initial of the second given name, and date of birth, a specific search may be done. In the majority of cases, this information will reveal the correct record. More frequently, however, a requester may only have the first given name and the surname. A search of this type may reveal a list of people with similar names in Ontario and their dates of birth, addresses and financial liability. When the PPSR system was being developed, a number of possible identifiers, including the SIN, were examined for their utility in limiting output to information queries. However, all other identifiers were discarded in favour of names and dates of birth, although it was recognized that names may be duplicated and dates of birth may be neither accurate nor easily obtainable.

Criticisms of the system focus on the interpretation of the purpose of the PPSR system, and on the balance between individual and public interests when considering whether disclosure of this kind of information represents an unwarranted invasion of privacy. Under Section 44 of The Personal Property Security Act, the registrar is permitted to provide information about anyone named in the PPSR file to anyone who requests it. Presumably, one of the purposes of this section is to enable a free flow of information among people who are involved in financial transactions. Credit reporting agencies are useful institutions in the business community, providing a benefit to both lenders and borrowers by supplying them with financial data about people with whom they may deal. This service is one which appears to be neither inconsistent with the law nor overly privacy-invasive. However, it would appear that privacy interests could be better protected by making debtors aware of the public accessibility of the PPSR system when their names are first registered on the file.

The possible use of information on the file for purposes other than establishing creditworthiness or protecting a security is a problem presented by all large, publicly accessible files. Taking all interests into account, the present loss of privacy resulting from a general search of the PPSR system is simply a cost associated with the establishment of a necessary facility.

The fourth issue, concerning the currency and accuracy of information within the file, poses a more serious privacy problem. At present, creditors are not required to update the register by filing a notice of discharge. Although debtors have the right under The Personal Property Security Act to demand that a discharge be provided after the debt has been paid, and penalties exist for non-compliance with such a request, consumer debtors are not in general aware of their rights and do not take steps to register a discharge. Therefore, information in the system is likely to become out-of-date when a loan is paid off. Without a statutory requirement that creditors send in discharge notices to the PPSR system, no real incentive exists for the creditor to report changes in file status.

LICENSED DRIVER AND VEHICLE OWNERSHIP RECORDS

Ontario licensed driver and vehicle ownership records are two other examples of government-held personal data available to the public. In addition to highlighting the problem of defining circumstances under which personal information should be made public, the investigation of these records brings into focus two other privacy issues: the use of government-held personal information for commercial mailing lists, and preferential access to government data banks by law enforcement authorities.

The Licensed Driver File

The licensed driver file, which is stored in computers, contains information on more than five million Ontario drivers. The application form for a driving licence requires individuals to provide their name, address, height, age and date of birth. When an Ontario driving licence is issued, the number contains a code representing the individual's surname, given name and middle initial, sex and month, day and year of birth. Each licence number is unique.

An applicant for an Ontario driving licence must complete the form designated for the particular class of vehicle he wishes to drive, among eight classes of vehicles described in the act. Three "medical grade codes" refer to medical condition[47], visual acuity and age. As well, applicants for certain types of driving licences must undergo criminal record checks[48].

The computer file does not contain any information from the criminal record (except information about traffic offences); it merely indicates that the record check has been done in accordance with the requirements of the act. Similarly, where medical certification is required, the computer record merely notes that the medical report has been received by the ministry. The contents of the report itself are filed in document form. Under the Highway Traffic Act, all medical reports are protected from disclosure[49].

The public licensed driver file also contains information on convictions for driving offences, demerit points resulting from such convictions, and suspensions and reinstatements of an individual's driving licence.

Three years of driver history information can be obtained from the file upon written request and payment of a \$3.00 fee which, the ministry maintains, deters the "merely curious." Specific information may be given over the telephone, provided that adequate identification is given by the inquirer. In 1976, there were one million requests for driver history abstracts from the general public. However, information about the driver's previous addresses are available only to government, law enforcement agencies, lawyers, and insurance companies concerned with matters involving a motor vehicle. Previous addresses are not otherwise revealed to the public in order to prevent use of this information by finance companies and collection agencies wishing to trace individuals. However, it should be noted that because inquirer identity is difficult to verify completely, some

personally sensitive information may inadvertently be revealed to these parties.

No logging mechanism exists to record the origin of specific inquiries or the identity of the inquirer. Therefore, no record subject could obtain a list of requesters, or even the number of requesters seeking access to his driving record during a given period of time.

Law enforcement agencies are accorded a greater level of access to driver registry data; they may obtain a typed copy of a complete five-year driver record, including convictions, driver status and information about suspensions and demerit points. In 1976, there were 160,000 requests for driver history abstracts from the police. Since 1978, police access has been facilitated by a sophisticated computer communications system. Five-year driver histories (excluding medical information) may be retrieved directly from the ministry computer by the Canadian Police Information Centre system (CPIC), which provides high-speed transfers of the information on request to 250 computer terminals in police stations and patrol cars throughout the province. Because of the information's availability at the time of an arrest, enforcement of licence suspensions has more than doubled since implementation of the CPIC-driver file connection.

Vehicle Registration System

Information on passenger vehicles and trailers is stored in computers. Information on all other types of vehicles (such as trucks and snowmobiles) is stored in a manual system. Both systems contain information on the type of vehicle, the owner, and the company with which the vehicle is insured. Listings of all vehicles currently owned by an individual or by a company, or descriptions of all vehicles owned by an individual or company in a given time period, may be obtained. Special computer programs may "call" the file of owners of a particular year and model of car.

As with the driver licence file, for \$3.00 per inquiry, anyone who makes a written request may obtain information from the vehicle file. To receive information by telephone, the inquirer's name and address must be previously listed with the ministry and inquiry fees paid in advance. Hospitals, universities, apartment building and parking garage owners attempting to control illegal parking, collection agencies, and investigatory agencies are among those permitted to receive telephone information, according to ministry officials. The list is maintained not to protect record subject privacy but rather to ensure that the ministry is duly paid for its services.

Police access to motor vehicle information is facilitated in two ways. It is available twenty-four hours per day, seven days per week, through a Ministry of Transport telephone connection for the exclusive use of the police; and, like driving licence information, it may be retrieved directly from the ministry computer by the police through the CPIC system.

Bulk information from the vehicle file was at one time sold for one cent per record to the R.L. Polk Company, which developed mailing lists for sale to businesses. However, in 1974, this practice ceased in response to public concern about use of government records for commercial purposes. The information now sold to the Polk Company in bulk lists new vehicle registrations, which are subsequently sold to automobile manufacturers for the purpose of recalling vehicles with mechanical defects. Auto parts manufacturers or retailers may also buy address lists, with owner's names deleted, for marketing purposes. Agreement not to use information for sales promotions or other purposes beyond that originally intended is specifically stated in contracts between the ministry and commercial companies.

CONCLUSIONS

General

Growth of Personal Record Collections

Personal records kept by government have grown rapidly in number and detail. Collections of records have accumulated as a direct result of the increase in the number of activities in which government has become involved over the years. Nearly every new service provided by government, and every new regulatory power granted to government, has meant the creation of yet another set of records about the people or the organizations for whom the service was intended or whose lives or businesses were to be regulated. Concerns for privacy have arrived late on the scene, at a time when government records already touch almost every aspect of our lives. The current emphasis on reducing government spending means that fewer large programs in new areas of government activity will be created; however, reduced government spending may also lead to more extensive collection of information about people, particularly where eligibility and need for service are subject to increasingly rigorous tests. An example of this pattern is the recently instituted requirement that Ontario Student Award applicants give permission for the Ministry of Colleges and Universities to have access to their income tax

records. In addition, greater use will be made of personal records in planning and research, as government tries to improve the effectiveness of its programs, or identifies new areas of activity.

Potential for Privacy Invasion

Although much information about individuals is collected and kept by provincial agencies, and lack of policy and careless habits have created the potential for privacy invasion in several areas, our research group concluded that the privacy of the majority of citizens has not as yet been seriously abused by government information-handling practices. There are no all-encompassing dossiers from which some mysterious force is extracting information with which to rule private lives. Citizens may feel at times that the forms they fill in are tedious and unnecessary, and they may wonder what happens to the information they provide, but in general Ontario residents can expect to be educated, to be granted credit and to own a house or drive a car without yielding many of their inner secrets, and without promoting privacy-intrusive activities by government agencies.

Principal problem area: recipients of government services

When people cease to be healthy, or self-supporting, or come to the attention of law enforcement agencies, their personal privacy may be jeopardized by giving up personal information to government. Insurance companies do attempt to verify health records; welfare officers do occasionally check car licence plates to see who is visiting whom; employers do sometimes check criminal records; and law enforcement authorities do collect information about some organized political groups.

In many cases there are quite understandable reasons behind these desires to collect personal information. Some people do try to defraud insurance companies; others try to cheat the welfare system; there are people who represent a definite risk, because of their past behaviour, in positions of trust; and some crimes are committed by organized groups who are prepared to engage in politically motivated violence. The problem is to determine where the balance lies between a legitimate need to know and the privacy of the individuals concerned and others who provide sensitive information contained in government-held records.

Growing use of computers in government

Most large government record collections, including those pertaining to health, licensed drivers and vehicles, student loans, law enforcement, corrections and income supplements are already stored in computer files. In many areas, major new computerization projects are planned or underway, and most agencies view the computer as a key element in a drive toward greater efficiency and improved management effectiveness. Although restraints on government spending in recent years may discourage rapid development of computerized information systems, the move toward computerization and the use of advanced communications technology is inexorable. The effect of this technology upon the privacy of Ontario citizens does not appear to have been completely assessed nor fully considered in decision making about automating record systems.

The impact of computers on privacy

The implementation of computerization can have both good and bad effects on privacy. Information can be assembled in a common format in one single location. This means that, although the technical expertise required is highly specialized, it is possible for a person with access to the computer file to rapidly scan the entire file and to extract data from it. However, centralizing data enables greater physical security to be maintained and the adoption of more foolproof techniques limiting the accessibility of data. For example, it is possible to automatically log use of the data, and to suppress portions of the data which should not be revealed for reasons of confidentiality.

There are, however, reasons why centralization of data in a computer bank can be a danger to individual privacy. A central data bank in which all the information is contained in a uniform format can be a tempting resource for more than one potential user, and the possibility of combining data banks which together form a much more useful profile than they do separately can be attractive. The potential for integrating various types of personal data is enhanced by wide and increasing use of the Social Insurance Number as a personal identifier. The need for some controls over potential privacy invasion by computer is apparent.

Areas of Concern

In a previous chapter, we identified the following areas of potential concern with respect to the protection of informational privacy:

1. public knowledge of data banks;
2. collection of personal information;
3. maintenance of the integrity and security of personal information;
4. transfer and dissemination of personal information;
5. subject access to personal information.

It is now appropriate to draw together the conclusions emerging from our survey of current practices about these topics.

Public Knowledge of Data Banks

There is no adequate overall listing or index of personal records held by the Ontario government, nor is there any regular reporting of developments in record-keeping and information systems. In the absence of an accurate, complete and regularly updated compilation, it is difficult for record subjects to ascertain what and where information about them is kept, and for interested members of the public to evaluate government record-keeping practices. This problem is particularly serious in the law enforcement area, where, in effect, secret data banks exist. The public has little knowledge of the types of intelligence and crime prevention activities or the extent of information collected in the course of such activities.

It appears, however, that there is sufficient internal administrative information about most records kept by various Ontario ministries and agencies for an overall index to be readily compiled. Most manual record collections have been scheduled for storage and eventual destruction, and the size of each record collection has been documented. In addition, each ministry makes an annual report to Management Board on the computer systems it has in operation or under development as part of the budget preparation process.

Absence of privacy-oriented policies on information collection practices

Although there appears to be a growing awareness of and sensitivity to the privacy issue throughout government, privacy considerations do not appear to have weighed heavily in the planning of information collection by government. Our research group's investigation of various government data banks revealed that personally sensitive information is routinely gathered by

several ministries, including those dealing with health, education, employment, social services, law enforcement and corrections. Some potentially privacy-invasive methods of collecting information, such as gathering information from neighbours and relatives, were also discovered. In the absence of policy guidelines, administrators have been left on their own to make judgments about what to collect and what not to collect, except where collection parameters were laid down specifically in statute or regulation. Decisions have therefore been based largely on the perceived need for information in the administration of a particular program. It should not be surprising that the objective of effective administration is pursued with vigour; yet there are dangers that administrators will lose sight of those privacy interests that create inconvenience or seem to be inconsistent with the overriding purpose of the program or activity. This is especially the case in the social services, where the fact that people are being helped is often seen as justification for invasions of their privacy, and in law enforcement, where it is argued that the objective of protecting society should take precedence over rights to privacy. Further, there appears to be a tendency, especially in the social services field, to engage in "fine-grained" decision making, or the making of decisions on the basis of very detailed criteria, which results in the gathering of sensitive personal information.

Maintenance and Security

Policies regarding retention and destruction of personal data have either been absent or inconsistently applied at the service delivery level. The quality of personal information often deteriorates over time, especially when it is automated. Although the Ontario Manual of Administration contains guidelines on the subject, and all ministries use retention schedules for records management purposes, neither the guidelines nor the retention practices are based on privacy considerations. It appears that no provincial program regularly destroys client records shortly after client service terminates in order to avoid the use of that record for "labelling" purposes. Uniform privacy-oriented policies for the destruction of personal records have not been developed in the Ontario government.

Technical data security is generally adequate, but personnel security practices often expose personal information to unauthorized use. Efforts are needed to ensure that a continuing awareness of the need for security is maintained. There are no overall standards for security of personal records held by the Ontario government. Similarly, there is no classification system for files or documents, although the Ontario Manual of Administration does contain minimum standard practices for the security of

operational computer systems and master files. A recent status check on systems integrity, which was carried out by a consulting firm on behalf of the Management Board Secretariat, concluded that security procedures for transaction origination, data entry, data communications and computer processing are generally adequate. The study also concluded that system controls in the government data centre examined are as good as or better than those employed by the average private sector computer centre. However, computer and telecommunications technology are advancing with such rapidity that the access and transfer of data by both licit and illicit means becomes cheaper and easier almost every day. At the same time, few incentives exist for the government to improve data protection. Implementing security measures was seen by many of those interviewed by our research group as expensive and time-consuming.

Technical security (that is, checks on computer system integrity, various system protocols, locked computer and telecommunications access points, and encryption) makes up only one facet of the security problem. Unauthorized use of data by authorized personnel is the weakest point in the security armour surrounding personal data. Our privacy research group's own observations confirmed that high staff turnover and use of private consultants contribute significantly to the security problem. Careless personnel practices, such as leaving personal records in unlocked drawers, filing cabinets and offices, taking records home, talking about clients over the telephone before checking the identity of the caller, and discussing client business in public areas were responsible for a number of security breaches. Contributing to this problem is a lack of sophistication in many Ontario government computer systems, which necessitates several manual steps prior to computerizing information, including copying information onto special forms, coding, keypunching, transporting to a computer facility, and inputting at a computer terminal. At each of these stages, personal records become less accurate and are more likely to be lost or misplaced. In fact, some officials in the social services area reported that forms are often lost during these processes.

In determining appropriate levels of security, it is obviously necessary to make an assessment of the possible uses which could be made of the data and their potential value to others. While many of the government's personal record collections would be of little use to anyone other than the staff of the program which gathers them, other collections could be of sufficient value to encourage outsiders to take unusual steps to gain access. The present controversy over unauthorized access to medical records is a case in point.

Transfer and Dissemination of Personal Information

The transfer of personal records among government record holders is not controlled by consistent policy. The majority of government officials interviewed stated that personal information maintained by them is confidential, except where public disclosure is permitted by statute or tradition, but our research group formed the impression that this protectiveness was more a result of official reserve than any strong concern for peoples' privacy. Several instances of regular, formal data sharing between the data banks of unrelated programs were found. One illustration of this is law enforcement use of motor vehicle and driver information, held by the Ministry of Transportation and Communications. Indeed, there is a considerable amount of information sharing by many non-justice programs with agencies in the justice field, and among justice agencies. A great deal of data sharing also takes place among social agencies and between social service and non-social service programs, particularly by word-of-mouth, but also by formal arrangements, such as transfer of school attendance records of welfare recipients to welfare programs. Few policies dictate exactly when and to whom these transfers are appropriate, thus increasing the possibility for individual decisions to transfer information which may violate the personal privacy of record subjects. The Ministry of Corrections is the only ministry studied that has formulated and implemented comprehensive rules regarding the transfer of personal information.

The most extensive sharing of sensitive information takes place in the social services. Apart from medical records, personal information collected by social services agencies is probably the most sensitive of any personal records collected by government. The sensitivity of such records results from the fact that reliance on social assistance, such as welfare, is seen by many to be a stigma and the fact that eligibility determinations often require ongoing surveillance of recipient's circumstances -- whether they are looking for work, with whom they are living and what they are buying. In an attempt to help individuals, social services agencies frequently collect subjective information about attitude and behaviour, which may involve discussions about applicants with employers, teachers and neighbours, and information sharing with other ministries such as Health and Education, often without the knowledge of the individual. There are signs of a growing awareness of the need to consider the privacy of the individuals with whom social service agencies deal. Our research group found the work being done in this area by the Children's Services Division of the Ministry of Community and Social Services to be most encouraging.

Breaches of confidentiality are most likely to occur at the working level. The greatest concerns for confidentiality were at

the managerial level. Although most of the operating or professional staff were aware of the need for confidentiality, there was more informal sharing of information at this level, often by word of mouth, among those with shared interests in a particular individual. The major controlling factor in the dissemination of personal information at this level is the fact that such sharing generally takes place only among members of what is perceived to be a "professional" group. Thus, social workers will share information with educators or other public servants. Confidentiality is, therefore, partly preserved by a sense of "professional ethics," rather than by any formal policy, although many of those interviewed mentioned the oath of secrecy which is sworn by all civil servants. The inherent dangers in this situation are that both the appreciation of the need for physical security in the handling of personal records and the qualifications for membership in the "professional" group authorized to receive sensitive information vary by individual record handler. (One employee questioned about the type of person who might fit the professional category replied that anyone carrying a ministry identification card would be permitted access to sensitive records. Over 20,000 people in the ministry examined carry such a card.) Furthermore, because sharing information among "helping" professionals is considered in the best interests of the client, the desirability of the record subject's prior knowledge of and consent to such transfers is frequently overlooked.

Notwithstanding the lack of controls over information sharing, the majority of government programs are quite distinct and separate from each other, leading to considerable duplication of information gathering and storage. The threat to privacy presented by this situation is that the individual requesting a number of similar government services may have to give up very sensitive information several times to several government employees. As one person interviewed stated, a certain "territorial imperative" is exercised over information; this raises intrinsic barriers to data sharing, even where such sharing would clearly be advantageous to the individual. This unwillingness to share data may, paradoxically, result in a related problem of privacy invasion: an over-integration of personal records among programs with dissimilar objectives (for example, rehabilitation and income maintenance programs).

In certain cases, the public interest in having access to records outweighs any privacy interest in suppressing them from public view. Three of the records systems held by Ontario government ministries for which individual access is totally open, and where the individual can obtain a copy of the record, are the driver and vehicle files in the Ministry of Transportation and Communications and the Personal Property Security Registration System in the Ministry of Consumer and Commercial Relations. All

three systems are also open to the public, however, and there have been questions as to whether the privacy of the subjects of the records is thereby invaded. In these particular cases, it seems clear that the public interest in having access to these specific records outweighs any privacy interests. Such situations highlight the tensions between freedom of information and privacy. The sale of lists of identifying information from driver or other government-held files also raises questions. We shall return to this issue in Chapter 37 of this report.

Subject Access

Most of the record collections examined are not accessible to the subjects of the records. The policy of confidentiality afforded personal record systems often is interpreted to mean that even the individual on whom the record was kept cannot gain access to it. While the majority of those interviewed by our researchers were in agreement with the general idea of individual access, many had reservations about permitting access to the files for which they were specifically responsible. They were aware of many actual requests received from individuals wishing to see their files; however, requests which had been received were usually denied. In nearly all programs examined, files were regarded as the property of the organization. The person concerned, therefore, was thought to have no rights regarding the information contained in the record. Where subjective information or information gathered about the person from others was likely to be included in the file, this reluctance about revealing the contents of the file was particularly acute. Also, many physicians and psychiatrists strongly resist any suggestion that they share clinical information with their patients. Concern was expressed that the opening up of access to personal records might significantly affect information collection activities. Some of these effects, such as more objective reporting of personal characteristics, may, of course, be beneficial. Many law enforcement officials believe that subject access must be restricted to avoid compromising third-party sources.

As we described earlier, at least one ministry has successfully implemented a broad subject access policy. Under section 231 of The Education Act, elementary and secondary pupils and their parents are granted full subject access and correction rights to their Ontario Student Records (OSR) stored at public schools. Despite a possible adverse effect upon teacher record-keeping practices, the subject access provision appears to have been successful in allaying many parental and pupil fears about the contents and uses of their educational records. While the provision has not been widely used, it may be that the mere

knowledge of the availability of files reassures the public of the propriety of educational record keeping.

CHAPTER 27 NOTES

- 1 See Volume 2, Chapter 8, Section F.
- 2 Canada, Treasury Board, Index of Federal Information Banks (Ottawa: Minister of Supply and Services Canada, 1979).
- 3 M. Brown, B. Billingsley and R. Shamai, Privacy and Personal Data Protection (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980) 25, cited hereafter as M. Brown.
- 4 Protection of Privacy in Ontario (Toronto: Ontario Law Reform Commission, 1968).
- 5 Interministerial Committee on Privacy and Computers, Report (Toronto: ICPC, 1973) 2, cited hereafter as ICPC Report.
- 6 Canada, Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972).
- 7 ICPC Report.
- 8 At the time, this legislation was pending before the legislature as Bill 101. A revised version was enacted as S.O. 1973, c. 97, proclaimed in force July 2, 1974. This legislation is described in Chapter 30 of this report.
- 9 ICPC Report, Appendix C.
- 10 Ibid., Appendix D. Government Services questioned the ministries of Labour (Human Rights Commission case histories), Education (student awards), Colleges and Universities (student awards), Health (OHIP claims, medical histories) and its own officials (government payroll/personnel).
- 11 Ontario Privacy Project Task Group, Report and Recommendations (Toronto: Management Board of Cabinet, 1976), cited hereafter as Task Group Report.
- 12 Health, Consumer and Commercial Relations, Colleges and Universities, Education, Solicitor General, Revenue, Transportation and Communications, Labour, and Community and Social Services.
- 13 Task Group Report, 6.

- 14 See Chapter 26 of this report.
- 15 See M. Brown.
- 16 O/R 38/73 amended by O/R 30/76, s. 2.
- 17 S.O. 1974, c. 109.
- 18 M. Brown, 430.
- 19 R.R.O. 1970, Reg. 749 as am., s. 74.
- 20 "Collective Agreements between Management Board of Cabinet and Ontario Public Service Employees Union Respecting Employee Benefits," October 1, 1977 to September 30, 1978, Articles 13.9, 13.10.
- 21 O/Reg. 173/63.
- 22 Ministry of Community and Social Services, 47th Annual Report for the Fiscal Year Ending March 31, 1978 (Toronto: September 1978) 6. "In total, there were 232,850 beneficiaries [of allowances under The Family Benefits Act in the fiscal year]."
- 23 For example, form 80-00-107, "Desertion Report," is used to obtain a detailed "Description and Information of Missing Person" (father), including eye colour, occupation, place of birth, height, weight, social insurance number, OHIP number, visible identification features, employer's name and address, and addresses and phone numbers of relatives and associates. The form also provides a large area for "comments" and the note "If applicant/recipient does not know this information (missing person's date of birth, social insurance number, etc.) it is usually obtainable from documents in woman's possession." Children's Services Division, Consultation Paper on Legislative Amendments (Toronto: December 1977) 38-40; Children's Services Legislation: Changes Resulting from Consultation (Toronto: June 1978) 15; Children's Services Legislation Summary (Toronto: June 1978) 18.
- 24 Children's Services Division, Consultation Paper on Legislative Amendments (Toronto: December 1977).
- 25 Children's Services Division, Report on the Task Force on Case Information Disclosure (Toronto: May 1979).

- 26 Children's Services Division, Children's Residential Care Facilities: Proposed Standards and Guidelines (Toronto: September 1978).
- 27 R.S.O. 1970, c. 351, as amended by S.O. 1972, c. 1, s. 97.
- 28 The term "law enforcement agencies" was broadly construed to include service agencies such as the Children's Aid Societies and the John Howard Society.
- 29 This account of information systems is based primarily on interviews with law enforcement officials, not on firsthand observations of the systems themselves.
- 30 See generally, "Canadian Police Information Centre," RCMP Publication 7610-21-876-3477.
- 31 "U.S. study finds most records err" (The Globe and Mail, March 6, 1977) 5.
- 32 Report of the Committee on Data Protection (Lindop Committee) (Cmd. 7341, 1978) 221, cited hereafter as Lindop Committee Report.
- 33 See, for example, Iowa Code, c. 692 (1974) s.9, which prohibits the maintenance by either manual or automated means of any "surveillance data," i.e. "...information on individuals pertaining to participation in organizations, groups, meetings, or assemblies where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person." [emphasis added]
- 34 New South Wales, Australia, Privacy Committee Act, 1975 No. 37. The committee undertook an examination at the request of the Premier of New South Wales of the security and intelligence files maintained by the New South Wales Special Branch, a counterpart of the OPP Security Branch. The committee reported in its findings that much of the file material was both privacy-invasive and unnecessary to legitimate security needs. Three months later, the Premier announced that 50,000 of the 80,000 files held by the Special Branch had been destroyed; see K.P. O'Connor, Federal Police Records, (Sydney: Australian Law Reform Commission, 1979).
- 35 Swedish Data Bank Statute (1973: 289).

- 36 Law no. 78-17 Concerning Data Processing, Files and Liberties.
- 37 Lindop Committee Report, 222.
- 38 No criminal record checks are undertaken by the OPP for private sector employers or for agencies not approved by the commissioner, although requests from such sources are continually received. Local OPP detachments also receive occasional requests for criminal record information, from, for example, local Children's Aid Societies regarding persons who have applied to become foster parents. In all cases, an individual's written approval is sought before a check is made.
- 39 For example, Wendy Herman, "Phone call opened police criminal files," (Toronto Star, July 14, 1978).
- 40 Chapters 6 and 29.
- 41 Prior to August 1, 1978, persons serving indeterminate or indefinite sentences in provincial institutions were subject to the jurisdiction of the National Parole Board. The Criminal Law Amendment Act, 1977 abolished indefinite sentences, and as a result the provincial board assumed responsibility for parole decisions about all inmates in provincial institutions.
- 42 For the year ending March 31, 1978 there were 61,834 admissions to detention centres and jails. Of these, 38,509 resulted in sentences to terms of imprisonment. A total of 14,387 persons were in custody in correctional centres during the year ended March 31, 1979. A total of 64,477 persons were under mandatory supervision during the year ending March 31, 1979, of whom 39,984 were placed there during the year. Parole applications totalled 5,440 for the year, and 1,968 persons were granted parole.
- 43 S.O. 1978, c. 37, s. 10.
- 44 The Parole Process (Ottawa: Law Reform Commission of Canada, Administrative Law Series, 1976).
- 45 R.S.O. 1970, c. 344.
- 46 The records are purged every three years, so that an address history beyond that period cannot be established.

- 47 The only medical information required to obtain an ordinary licence indicates whether the applicant is subject to epilepsy, convulsive disorders, dizzy spells or any condition that causes unconsciousness. In such cases, the individual may be required to obtain a fuller medical report from one or more physicians.
- 48 The most searching examination is made for school bus driver applicants, who must undergo a medical check, as well as a criminal record check made by the Ontario Provincial Police criminal records branch to determine whether the individual has been convicted of a morals charge or of drug trafficking or use. According to ministry officials, a criminal record check for driving instructors will also be included in the regulations in the near future.
- 49 R.S.O. 1970, c. 202, s. 143(3). In addition to the information given by the record subject during the application process, medical information is independently generated by doctors and optometrists (who must report to the registrar the name, address and clinical condition of every person sixteen years of age and over who suffers from a physical or mental condition, including habitual drunkenness or narcotic addiction, that may make it dangerous for him to operate a motor vehicle) and by non-medical sources, such as concerned family members.

Personal Identifiers: The Development of a Single Identifying Number

Various terms are used to describe the different ways in which people are identified when information about them is recorded. These "identifiers" have traditionally served three purposes within record systems. First, they identify each individual's record, separating it from others. Second, they provide an easy means of locating an individual record for use or updating. Third, they may be used to index personal records. In our discussion, the terms used are: unique personal identifiers or UPIs (numbers, letters or symbols unique to each individual whose record is contained in a system); standard identifiers (such as name, address and age); single identifying numbers (single numbers identifying a person in all record systems where information about him is stored); "personal registration numbers" or "universal personal identifiers" (numbers assigned to persons at birth or upon immigration to a country); and the Social Insurance Number or SIN (the nine-digit number widely used since its inception in 1964 under the Canada Pension Plan Act[1]).

A. THE CHANGE FROM "STANDARD IDENTIFIERS" TO UNIQUE PERSONAL IDENTIFIERS

Standard identifiers (such as names and addresses) have traditionally been used in large record systems. However, as more records are kept, and for longer periods, standard identifiers are increasingly inadequate for a quick one-step search. The use of such identifiers often yields a number of possible records which must be sifted, using other information in order to locate the correct one[2]. In many systems, further checking can be costly and time-consuming. Accordingly, many organizations have assigned Unique Personal Identifiers to individuals, accounts or cases to facilitate the operation of large record-keeping systems.

UPIs have two principal advantages. First, they assist in establishing that a person with a given "standard identifier" is in fact the correct person. With the computerization of large record systems, the argument for initiating unique identification to eliminate cross-checking or manual verification in order to improve search efficiency is reinforced. Second, UPIs have a distinct advantage over other types of identifiers in the area of privacy protection. Because an individual is less likely to be confused with another, he is unlikely to be blamed for another's

misdeed, or sought after by a government agency or other organization seeking another person with a similar name or address. UPIs may be designed to be unique to a particular system. Most residents of Ontario could list many UPIs generated in their contacts with governmental institutions, banks, credit-granting institutions and retailers. Where the records in one system are retrievable by identifiers unique to that system, prospects of being matched with records in another system are reduced. This type of UPI permits the maintenance of some degree of anonymity as the individual comes into contact with various organizations throughout his life[3].

However, when the same UPI is used by several separate agencies with different objectives, the problems of potential loss of record subject privacy through data linkage arise. The UPI then threatens to become a single identification number, and raises concerns that it may be used by governmental and non-governmental organizations to build up "dossiers" of personal information drawn from various data banks using the number as an identifier.

B. SINGLE IDENTIFYING NUMBERS

The chief advantage of a single identifying number over other means of record identification is that it can be used to facilitate record linkage. In the same way that UPIs in a system permit better file identification for record access, a universal single identifying number permits more efficient "interface" of personal data systems. This interface promotes greater accessibility to personal information systems, and in effect creates a single system by making it possible to merge information in several different systems, without physically moving the data banks together.

The benefits accruing from this are many: the increased information base available (from merged data systems) for government program decision making; less duplication in information gathering; and an expanded information base available for statistical use in research, planning and administration.

There are also two potential benefits to the individual about whom records are being maintained: the benefits of more accurate record keeping, and the ease of dealing with just one organization, instead of many, to retrieve personal records, provide information for correction or updating, or to track and control record dissemination. However, it must be realized that such benefits can only accrue to the individual if systems are designed to provide them. The majority of the data systems examined in the

course of the Commission's research program provide none of these benefits to record subjects. Thus far, proposals for single identifying numbers to be used by government have been based on improved administrative efficiency, rather than on any direct benefit to the individual.

There are two basic arguments against the use of a single identifying number. The first is that the use of numbers (instead of, for example, personal names) is a dehumanizing influence on government administration, and on all large, seemingly faceless organizations. As far as this position is concerned, the single identifying number issue may be simply one of many aspects of the problem of remoteness in our institutions, and, in fact, one of the less important ones. If large organizations were more approachable, flexible and open in their dealings with the public, then perhaps the single identifying number would not be seen as such a threat to human dignity, but rather as a neutral tool of administrative technology. Such considerations are part of a larger debate than is possible within the context of this report.

The second argument is that use of such numbers will facilitate invasions of privacy or intrusions into private lives because of an enhanced ability to link data bases into what could effectively be a national data bank of dossiers on every resident. The linkage of different record systems and the exchange and consolidation of information about people is not always beneficial to the individuals concerned[4].

The possibility of this kind of linkage also gives rise to the fear that dossiers could be used to follow people throughout their lives, and might lead to or facilitate repressive forms of social control. Where the individual has committed an act of wrongdoing in the past, data linkage might prevent him from making a "fresh start."

Both these arguments against the use of single identifying numbers are based on a justifiable concern about the use of data for a purpose different from that for which it was collected. The risk of what is referred to in the Canadian Human Rights Act, Part IV as "non-derivative use" of personal information may be heightened by the enhanced ease of data sharing through a single identifying number. However, this problem would not be resolved merely by banning single identification numbers. Rather, its resolution lies in the enactment of data protection rules which prohibit certain types of record transfers for unconnected purposes, and which require subject authorization prior to any record transfers from the original source of record collection.

The controversy over use of single identifying numbers is just one component of the issue of data protection. Data identification is already quite sophisticated, and data linkage may be satisfactorily accomplished without the use of single identifying numbers.

C. PERSONAL IDENTIFIERS IN THE ONTARIO GOVERNMENT

Ontario government programs use a variety of methods to identify and authenticate records: standard identifiers such as name, address or birthdate; specific application identifying numbers (UPIs) such as driving licence numbers, vehicle licence numbers, and birth identification numbers; case numbers such as those used in social services and certain health programs; and OHIP and Social Insurance Numbers.

In the majority of record systems, more than one identifier is collected, even if they are not all used for record retrieval purposes. Records are often filed by name, but a number (such as a case number) serves to verify that every record added to the file applies to the correct person. In large record systems (particularly automated systems), records are filed by both name and UPI. For example, in the computerized government employee information system records are filed by both name and SIN, and in the driver licensing system by both name and driving licence number. The flexibility of data base technology makes it possible to store and retrieve individual records by using any of several identifiers.

Particularly in large computerized systems, use of more than one identifier can be an important safeguard for the individual, ensuring that information is recorded in his file and not in someone else's. This is why the most extensive range of identifiers is collected by law enforcement and corrections agencies. In addition to physical description, these agencies collect driving licence numbers, SINS and fingerprint identification numbers.

One exception to this use of UPIs for verification purposes is the Personal Property Security Registration system (PPSR), which, although very large and volatile, identifies records only by name and address. The policy of not using unique identifiers has led to some criticism because general inquiries of a name can yield a long list of record entries (for example, all the John Smiths on the system), which may be seen as an invasion of privacy. (The PPSR is described in Chapter 27 of this report.)

The two most common numbers collected, according to the 1976 Ontario Privacy Task Group[5] are the SIN and the OHIP number. The OHIP number is, of course, used primarily in health or medical areas, but social assistance providers and OHIP subscribers, such as government employers, also record the number to facilitate linkage with the health insurance system.

D. THE GROWING USE OF THE SOCIAL INSURANCE NUMBER

Social Insurance Numbers (SINs) were originally established for the purpose of administering the federal unemployment insurance scheme instituted in 1936. Their adoption for use in tax collection and pension disbursement under the Canada Pension Plan was introduced in 1965[6] only after considerable parliamentary debate concerning the proposed new uses of the numbering scheme. Members of the opposition expressed concern that the use of the SIN might ultimately develop into a national numbering system.

The Pearson government included a section in the Canada Pension Plan Act which specifically assured individual contributors and beneficiaries that personal information communicated to personnel administering the act will be considered "privileged," i.e., not to be revealed to anyone except employees in five specified departments "where it is necessary to do so for the purpose of the administration of this Act"[7].

Since 1965, amendments to this section have extended the list of departments and other bodies allowed to exchange social insurance information[8], and have extended permissible use of the data to the administration of the Unemployment Insurance Act. Further, provinces are now permitted to use federally collected social insurance information to administer and enforce health insurance legislation[9].

Although it has periodically been expanded, the list of departments and agencies authorized to receive SINs under the Canadian Pension Plan Act may be more effective in protecting privacy than are the two confidentiality sections of the Unemployment Insurance Act[10]. The first of these sections gives the Minister of Employment and Immigration discretionary powers to release information obtained by the Unemployment Insurance Commission or the Department of Employment and Immigration (including SINs) "to such other persons as the Minister deems advisable...." The second permits the Unemployment Insurance Commission to make SINs available "for the accurate identification of individuals...to such persons as the Commission thinks appropriate to accomplish such purpose." Evidence presented to the

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police indicates that this broad discretion to disclose was exercised so as to permit access by the RCMP to information maintained for purposes of administering the unemployment insurance scheme, including the central Social Insurance Number Index. This practice was discontinued in 1978[11].

Personal information (such as address, relatives' names and employment history) contained in the index and on file in regional offices of the Unemployment Insurance Commission was, according to this evidence, used by the RCMP to identify and track down suspects.

Of far greater significance for the growth of SIN use, however, is the proliferation of use of the number by organizations maintaining personal data banks in federal and provincial governmental institutions and in the private sector. The confidentiality provisions of the Canada Pension Plan Act and the Unemployment Insurance Act regulate, in some measure, disclosures of personal information by governmental institutions engaged in the administration of the federal pension and unemployment insurance schemes. They do not in any respect restrict the ability of other governmental or non-governmental organizations to request their clientele to supply SINS and to use them for record identification and verification purposes in their record-keeping systems.

Thus, despite the original limitations and assurances concerning proposed use of the SIN, the use of the number for purposes quite different from those originally anticipated has become common in both federal and provincial government record systems. Most provincial health, education, personnel, law enforcement, corrections and social services programs use the SIN in establishing their personal record files. In many cases, the number is required for tax or payroll purposes. In others, it appears to have been collected precisely because of its anticipated future use as a universal single identifying number. The Commission's research staff was told by many government officials that space for a nine-digit number had been provided on forms in the expectation that use of the SIN would be adopted. Many administrators believed that a single identifying number such as the SIN would be desirable for the efficient administration of programs.

The federal government has also engaged in this expanded use of SINS. Many federal ministries and agencies use SINS to index their personal data systems[12]. One indication of the extent to which federal agencies have adopted the SIN as a single identifying number is the fact that individuals are required to use the number in gaining access to their personal files in the

majority of data banks listed under the Canadian Human Rights Act, Part IV[13]. In October, 1978, National Health and Welfare Minister Monique Begin commented that:

Canadians should expect their Social Insurance Numbers to be more widely used as identification in the computer banks of government and private industry...[This is] a policy of common sense...[14].

If these trends continue, it seems very likely that the SIN will be used as a de facto universal single identifying number in government personal data banks.

The widespread adoption of the SIN has not escaped public attention, nor has it been accomplished without opposition. One parent, for example, fought and won a battle with his daughter's local school board and her university over their required registration of pupils by Social Insurance Number[15]. A similar protest against a Canada Employment and Immigration Commission letter encouraging early pupil acquisition of Social Insurance Numbers for use in "organized sports and activities such as hockey, baseball, Air Cadets of Canada and Sea Cadets of Canada," was voiced by a group of Frontenac County parents[16]. In another recent dispute over use of the number, Ontario gun owners won the right to refuse to include their Social Insurance Numbers on applications for Firearms Acquisition Certificates. The Consumer's Association of Canada presented to former Minister of Revenue Walter Baker a resolution opposing the proliferation of use of Social Insurance Numbers[17]. The media have also been critical of increasing governmental use of SINs to index police records, public health records and sensitive Manpower files, and to register infants born in Prince Edward Island[18].

Private sector use of SINs is also increasing. Customers may be required to present their Social Insurance cards in order to cash or write cheques[19], buy and sell savings bonds, deposit and withdraw money in Registered Home Ownership and Registered Retirement Savings Plans, open bank and credit card accounts, receive private hospital treatments[20], and reserve airline seats on chartered flights[21]. One of the more controversial private sector uses of the numbers is their inclusion on employee badges[22]. The federal Privacy Commissioner for the Canadian Human Rights Act, Part IV, has received numerous inquiries about the use of SINs, the overwhelming majority of which were complaints about collection of the number by businesses -- particularly banks, insurance companies and employers.

The reasons for this increasing scope of SIN use are not difficult to discern. In part, the use of the number by public

and private institutions engaged in the provision of pension or other income-related benefits to members of the public is designed to facilitate confirmation of income by the Department of National Revenue. More generally, however, the proliferating use of the number is simply due to its convenience. Any large record-keeping system requires a method to identify each individual on file in the system. As we have indicated, the use of numbering systems is more efficient than other techniques of identification. Rather than establish new numbering systems for each new personal data bank, organizations find it more cost-efficient to use the SIN.

To what extent, then, does this phenomenon of increased SIN use represent a threat to the information privacy values identified earlier in this report? First, the prospect that the SIN may come to be used as a de facto national identification number is gradually becoming a reality. It is evident that more and more governmental and non-governmental organizations are using the SIN as an identifier in both manual and computerized personal information systems. However, it is not at all clear that the problem of data linkage and dossier building has become a widespread phenomenon. Our own inquiries have been limited to an examination of certain personal record-keeping systems of the government of Ontario and, accordingly, do not provide a basis for generalizations as to the extent to which data linkage is occurring in other record-keeping contexts. As far as Ontario practice is concerned, however, we are not aware of any plans to integrate all SIN-based information systems into a centralized personal information data bank. To the extent that linkages between data banks do occur, however, it is evident that widespread use of the SIN makes such exchanges more efficient and accurate.

The use of the Social Insurance Number by federal governmental institutions and by non-governmental organizations within the legislative authority of the Parliament of Canada is currently under investigation by the federal Privacy Commissioner pursuant to the terms of reference of a study commissioned by the federal Minister of Justice. The Privacy Commissioner has been asked to examine the following matters:

- a. the extent to which the Social Insurance Number is collected and used by those corporations, organizations, institutions, governments and other bodies within the scope of the study;
- b. the purposes for which the Social Insurance Number is used;
- c. whether or not the Social Insurance Number is used as a data-linkage device and, if so, the extent and implications of such use;

- d. whether or not the collection and use of the Social Insurance Number presents a threat to the privacy of individuals and, if so, the nature and extent of this threat;
- e. the possible implications of the regulation and prohibition of the collection or use of the Social Insurance Number.

The Privacy Commissioner is required to submit a report on these matters before August 1, 1980.

The growing use of identification numbers is not only a Canadian phenomenon. The use of such identifiers and its regulation have been a topic of discussion in many developed countries. In Chapter 36 of this report, we shall indicate the nature of the treatment the subject has received in other jurisdictions and consider possible methods of controlling its use by the Ontario government.

CHAPTER 28 NOTES

- 1 Material in this chapter is drawn in large part from M. Brown, B. Billingsley and R. Shamai, Privacy and Personal Data Protection (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980), hereafter cited as M. Brown.
- 2 For example, all "Smiths" in a file would have to be searched using some other characteristic in order to find a particular "Smith." Depending on the precision of an identifier and the time lag between data entries (some identifiers, such as addresses, change frequently), the "hit-rate" (the number of initial positive confirmed identifications not requiring further checking) can vary tremendously.
- 3 The privacy-protection ability of a UPI is further improved if the identifier chosen is meaningless in itself, that is, if it bears no relationship to any data, individual characteristic, or program characteristic.
- 4 Such linkage, exchange and consolidation of information is, of course, quite possible without a single identifying number. The method for identifying individuals by using a combination of standard identifiers or "natural" variables, such as age, sex, income and profession, where unique identifiers are not recorded, is called "backwards identification." For an explanation of the computer techniques used and their statistical probability of success, see Lars Olsson, Backwards Identification (Stockholm: National Central Bureau of Statistics, 1975).
- 5 Report and Recommendations (Toronto: Privacy Project Task Group, July 1976) 24.
- 6 Canada Pension Plan Act, S.C. 1965 c. C-5, s. 100. The original Social Insurance Number registration system actually came into effect one year earlier, under the regulations of the Unemployment Insurance Act, R.S.C. 1955.
- 7 Canada Pension Plan Act, S.C. 1965, c. 51, s. 107. The bodies authorized to exchange such information were the Department of National Health and Welfare, the Department of National Revenue, the Department of Finance, the Unemployment Insurance Commission and the Dominion Bureau of Statistics.
- 8 Canada Pension Plan Act, R.S.C. 1970, c. C-5, s. 107(3)(e.1) (4), as amended by R.S.C. 1970 (2nd Supp.) c. 33, s. 1.

- 9 Canada Pension Plan Regulations, P.C. 66-580, s. 802.
- 10 Unemployment Insurance Act, S.C. 1971, c. 48, s. 114, as amended by S.C. 1977, c. 54, s. 60.1. The second provision is contained in S.C 1971, c. 48, s. 126(4).
- 11 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Mr. Justice David C. McDonald, Chairman, Hearings (testimony beginning June 20, 1978) Vol. 57 and 58. Also see Jeff Sallot, "How the Mounties got a direct line to your SIN file," The Globe and Mail, September 20, 1978; and Jeff Sallot, Nobody Said No (Toronto: James Lorimer, 1979) 170-76.
- 12 These include the RCMP, CIDA, the Post Office and the department of Agriculture, Consumer Affairs, Defence, External Affairs, Fisheries, Health and Welfare, and Indian and Northern Affairs.
- 13 Canada Treasury Board, Index of Federal Information Banks: 1979 (Ottawa: Minister of Supply and Services Canada, 1979), and Government of Canada, Record Access Request Form (Canadian Human Rights Act, Part IV, form no. TB/CT 350(12/77)).
- 14 Edward Mann and John Alan Lee, RCMP v. The People (Don Mills, Ont.: General Publishing Co., 1979) 169-70, quoting The Globe and Mail, October 28, 1978.
- 15 Paul Shaver, letter to the Commission on Freedom of Information and Individual Privacy, January 10, 1979; and "Social insurance numbers are possible invasion of privacy, some fear," The Globe and Mail, September 19, 1978.
- 16 Letter to the Commission on Freedom of Information and Individual Privacy, December 20, 1978.
- 17 "Ottawa has promised action on CAC complaint about SINs," The Globe and Mail, December 6, 1979.
- 18 Jeff Sallot, "Even babies get SIN as clever idea grows and grows," The Globe and Mail, September 19, 1978.
- 19 For example, the Hudson's Bay Company Ontario stores specifically request Social Insurance cards from customers paying by cheque. The number is compared to a computerized system list of bad cheque-writers filed and indexed by Social Insurance Number.

- 20 Private hospitals in the Toronto area, for example, collect Social Insurance Numbers from all prospective patients and send records indexed by the number to a computer firm in the United States for regular statistical compilation.
- 21 Ken Romain, "Mandatory SIN bothers air charter industry," The Globe and Mail, December 14, 1978.
- 22 "Union seeks to block use of worker's SIN on CGE plant badge," The Globe and Mail, December 12, 1978.

CHAPTER 29

Data Protection Laws of Other Jurisdictions

A. INTRODUCTION

Although privacy protection problems have only recently become matters of legislative action, a number of jurisdictions in industrialized Western countries have moved to adopt privacy protection laws of one kind or another. In this chapter we shall examine the major kinds of legislative schemes enacted to deal with the informational privacy issue as it arises in the context of the operation of personal data information systems by public institutions. Although the legislative formats and institutional structures vary from one jurisdiction to the next, similar solutions have been adopted to reconcile the conflict between the individual's interest in privacy protection and the need for public institutions to collect, store, use and disseminate personal information. In essence, each of these schemes establishes machinery for the implementation of the principles of fair information practices identified in Chapter 25.

Given the wealth of comparative legislative material available to us, it has been necessary to be selective in our discussion. Primary emphasis will be placed on the data protection schemes of Sweden, the United States of America, and Canada. As well, reference will be made to the schemes in place in various European jurisdictions and in state jurisdictions in the United States, and to the activities of the New South Wales Privacy Committee. In describing these schemes, attention will be drawn to problem areas of particular interest, such as public knowledge of the existence and nature of government-held personal data banks; collection of personal information; maintenance of data integrity and security; control over transfer and dissemination of personal information; granting of subject access and correction rights; and development of computerized personal record-keeping systems.

B. SWEDEN

With the enactment of the Data Bank Statute of 1973, Sweden became the first nation to enact a statutory data protection scheme. Under the act, the establishment or continuance of a "register of persons" by any public authority or private

institution, such as a business corporation, is subject to monitoring by the Data Inspection Board (DIB), a supervisory agency established by the statute[1]. The DIB consists of a chairman, who may decide matters of lesser importance by himself, and eight other members. The board maintains a staff of approximately twenty-five civil servants. A "register of persons" is an information system for monitoring personal information by means of automatic data processing. Permission must be sought from the DIB to operate such a register. Details of the system must be submitted for a determination of whether an "undue encroachment on the privacy of the individuals registered" will result from the system's operation[2]. The application for a licence must include a description of the origin of the information destined for the register, and the means by which it will be collected[3]. When the approval of the DIB is granted, a licence is issued. Although the law applies to both private and public sector data operations, registers established by executive or legislative order are subject only to advisory opinions from the DIB, and need not get the board's approval. Apart from such cases, however, government data banks can be established only with the permission of the DIB.

Once a particular system has been approved by the board, a "registrar-accountable" must be named within the organization maintaining the register[4]. That person is responsible for the lawful operation of the register in accordance with the terms of the licence. The DIB establishes those terms by means of regulations dealing with the following matters:

1. the collection of information to be included in the file;
2. carrying out electronic data processing procedures;
3. technical equipment;
4. the scope of the data processing that may be performed on personal information in the file;
5. notice to be sent to persons affected regarding the uses made of the information;
6. the types of personal information which may be disclosed;
7. distribution and other uses which may be made of personal information;
8. maintenance and deletion of information;

9. control and security[5].

The responsibility for operating the register of persons within the regulations set by the Data Inspection Board and without unduly encroaching on the privacy of individuals, falls largely to the registrar-accountable[6].

The primary responsibility of the DIB is the regulation of personal data registers. The board may change the regulations under which a register operates, or revoke permission to operate a register. Both the design of regulations and decisions to revoke permission are based on the criterion of "undue encroachment on privacy"[7].

An appeal may be taken from any decision of the DIB to the King in Council. In such cases, the Attorney General may represent the public interest[8].

Certain types of sensitive personal information may not be stored in a register of persons by anyone "other than an authority responsible by law or statute for keeping a record of such information, unless there are extraordinary reasons therefor"[9]. This kind of information includes criminal or psychiatric records, social welfare assistance records, and health records. Registers containing information on political or religious views will only be permitted where there are special reasons for it.

The length of time the data may be stored is also regulated. Although the Data Bank Statute makes no specific reference to timeliness of data, the regulation requires the applicant to state how long records will be preserved, and how and when the "weeding" will be undertaken[10]. Timeliness becomes a condition of the licence granted by the Data Inspection Board, and administered by the registrar-accountable.

The general rules on subject access and correction are stated in the Data Bank Statute itself, whereas provisions for transfer of personal data to third parties may be set forth in the particular licence. The administrative responsibility for implementing these rules falls on the registrar-accountable.

Section 10 of the act entitles the individual to know what information exists about him on the record. Presumably a person possesses this right in relation to each register containing information about him. Requests for information are made to the registrar-accountable who must reply "as soon as possible," but he need only comply with such a request from the same person once every twelve months. Exemptions to the general principle of subject access are provided for by subsection 10(3), which states

that there is no obligation to release information if a "law or statute or the decision of an authority" forbids release to an individual.

A person who has obtained access to a file may become aware of incorrect information, and may wish to invoke the statutory duty imposed on the registrar-accountable to correct it. There are no statutory procedures for the correction of data or for resolution of disputes about the accuracy of data; however, when the regulations relating to the register are established, procedures for access and correction may also be devised. Section 8 of the act states that if there is "reason to suspect that information on persons is incorrect, the registrar-accountable shall without delay take the necessary steps to ascertain the correctness of the information...." Corrections made in this way are to be transferred to previous recipients of the information.

The registrar-accountable is also charged with ensuring the completeness of information contained in the register. Section 9 provides that "the registrar-accountable should undertake what is necessary to complete a register of persons if the information on persons with regard to the purpose of the register must be regarded as incomplete..." [emphasis added]. However, if the lack of completeness may result in an undue encroachment on privacy or a risk of loss of rights, the section requires that "such completion must always be undertaken..." [emphasis added].

Although the question of third-party access to personal files is dealt with by the DIB on a register-by-register basis through the terms and conditions of specific licences, a few provisions in the act impose limitations on such access. Section 11 forbids release of information "if there is reason to believe that the information will be used for electronic data processing without permission in accordance with this statute." Transfers abroad depend on permission from the DIB, which will not be granted if the transfer may result in an "undue encroachment" on privacy. As indicated above, if information has been released to a third party, Section 8 provides that the data subject may request that any deletions or changes in the data since its release be reported to the third-party recipient. Further, the specific regulations governing a particular register may state that a third-party recipient of information from the licensed register may not pass it on without authorization.

The act provides a variety of sanctions for breach of duty. A register of persons established without permission may be "declared as forfeited"[11]. The maintenance of incorrect information in a register may result in damages being payable by the registrar-accountable to the data subject[12]. Denial of access

to the DIB to premises where a data register is kept, denial of requests for information from the board, or breaches of other duties may result in fines being assessed against the registrar-accountable by the board[13].

The act also establishes general offences pertaining to the unlawful establishment or operation of a register of persons; the violation of a regulation promulgated for the operation of a register; the unlawful release of personal information; the delivery of incorrect information either to a data subject or to the DIB; and the release of personal information or professional or business secrets, knowledge of which is gained through dealing with a personal register[14]. Persons convicted of such offences are subject to a fine or a term of imprisonment not to exceed one year. The quantum of the fine is not limited by the statute. The act further provides that proceedings shall be instituted by the public prosecutor only where the aggrieved person requests it, or when the public interest calls for it. The more serious offence of "data trespass," or the effecting of unauthorized access or the making of improper alterations, deletions or additions to the records held in the register, is also established by the act. The penalty upon conviction may be a fine or imprisonment not exceeding two years[15].

In short, the Swedish Data Bank Statute sets out a comprehensive scheme of data protection, regulating the collection, storage and dissemination of personal data in computerized form by private and public institutions. The primary administrative mechanisms for the implementation of the statute are the Data Inspection Board and the registrar-accountable. The sanction provisions of the act give the DIB the power to penalize the registrar-accountable if the latter does not comply with the statutory duties. The ultimate appeal body for decisions taken by the board under the act is political -- the King in Council. Added to this, as we have seen, is a comprehensive code of civil and criminal liability for prohibited practices relating to the operation of personal registers.

In 1976, the Committee on Data Legislation (DALK) was commissioned by the government to undertake a study of the operation of the scheme. The resulting study, published in 1978, was generally favourable in its assessment and did not recommend significant departures from the essentials of the scheme outlined above[16].

C. OTHER EUROPEAN LEGISLATION

In the years following the enactment of the Swedish data protection law, most other Western European nations followed the

Swedish lead in regulating personal data practices. Further, international European organizations and committees have actively encouraged this activity, and have moved to standardize these laws[17]. For example, the Council of Europe passed resolutions in 1973 setting out principles of data protection and proposing international conventions accepting these principles. To date, the German Federal Republic, France, Luxembourg, the Netherlands, Austria, Norway and Denmark have adopted data protection laws.

Although Great Britain has not adopted such a scheme as yet, two major studies of privacy protection issues have been completed: the reports of the Younger Committee on Privacy (1972)[18] and the Committee on Data Protection (1978). The latter report will be discussed later in this chapter.

The European legislation, as a general rule, applies to data processors in both the private and public sectors, and usually requires data processors to be registered with or licensed by the government. Individual data subjects generally acquire rights of access, correction, and other means of control over uses made of personal data concerning them. Although there are basic similarities in the European legislation, important distinctions may also be noted, primarily with respect to the range of information systems and institutions covered by the acts and the administrative structures established to implement each scheme.

NORWAY

The Norwegian law covers both manual and automated personal information systems, although in the case of manual systems only those containing particularly sensitive personal information are brought within the scope of the data protection scheme. The act defines "sensitive personal information" as that relating to race, political or religious beliefs, law enforcement, health and alcoholism, sexual life or family matters[19]. Further, the statute embraces within the definition of "personal information" information concerning associations and other legal persons[20]. Licensing and regulatory powers with respect to all data systems covered by the legislation are vested in the King, although these powers may be delegated to the Data Surveillance Service (DSS), an advisory body established under the statute[21]. Personal data systems maintained by both private and public institutions are covered by the scheme. Separate licensing schemes are established in the act for private institutions engaged in credit reporting, data processing, mailing and addressing services, and the polling of public opinion[22]. With respect to the public sector, both central and local governmental institutions are covered by the

act. As in Sweden, a licence is not required for a personal data system expressly established by a separate statute[23].

DENMARK

In Denmark, two statutes were enacted in 1978: one governs private sector data processing either by automatic or "systematic" means, and the other regulates the use of computerized personal information systems within government. The latter statute establishes data protection rules to which a government system must conform before it is approved. With respect to the private sector, substantive rules are set out in the statute, some of which may be directly enforced by a regulatory authority established under the statute. It is only with respect to commercial suppliers of personal information that the authority's permission must be obtained prior to establishing the record system[24].

FRANCE

France enacted its Law Concerning Data Processing, Files and Liberties in January 1978[25]. Although various provisions of the law apply to both automated and manually processed personal data, and to both public and private institutions, the most rigorous controls established by the statute are applicable to the public sector. The act established a National Commission on Data Processing and Liberties, an independent administrative authority exercising regulatory powers over personal data processing and enforcing the data protection law through licensing and investigatory activities. The act itself sets out a number of fair information practices rules which must be adhered to by private and public institutions processing personal data.

Under the French scheme, only government data banks must obtain a licence from the National Commission in order to conduct personal data processing operations[26]. As far as the private sector is concerned, organizations engaging in automatic processing of personal data must register with the commission and give an undertaking that the processing will satisfy the requirements of the law. However, permission to commence operations is not required[27]. Article 17 of the act provides for a more abbreviated form of registration for processing operations undertaken by either public or private institutions "that obviously do not affect private life or liberties." The commission is obliged by the statute to make available to the public a list of licensed and registered personal data processing systems[28].

The composition of the commission was a matter of some controversy during the formulation of the scheme. Ultimately, it was determined that the commission should consist of seventeen members, twelve of whom are elected (two each by the Assembly, the Senate, the Economic and Social Council, the Conseil d'Etat, the Supreme Court of Appeal, and the Audit Office), in addition to five members who are appointed on the basis of their competence and expertise (one each by the president of the Assembly and the Senate, and three by the government). Members of the government or individuals playing a responsible role or owning shares in a data processing or telecommunications enterprise are not eligible for membership on the commission. The commission is described in the statute as an "independent administrative authority," and it is specifically provided that the commission shall not "receive instructions" from any other authority[29].

THE GERMAN FEDERAL REPUBLIC

A comprehensive data protection scheme was enacted in the German Federal Republic in 1977[30]. The general premise of the law is that processing of personal data is permissible where "expressly authorized by statute," or with the written consent of the data subject[31]. Automatic data processing and some manually-kept files are covered by the law[32].

Statutory obligations vary according to the identity of the data processor and purpose of the operation. Three groups of processors identified are:

1. authorities and other public agencies of the Federation, corporations directly under the Federation, institutes and foundations of the public law, and associations of such corporations, institutes and foundations;
2. natural persons, legal entities, corporations, and other personal associations of private law whose data processing operations are for their own business purposes;
3. the groups named in paragraph 2, where the data processing operation is for the benefit of third parties[33].

The statute is designed to yield to provincial (Länder) legislation[34]. A federal commissioner administers the act in relation to the groups named in paragraph 1 above; provincial supervisory authorities are responsible for the other groups. Authorities and public agencies must publish specified details about stored personal data in the Official Gazette[35]. Police, military and revenue authorities are exempt from this requirement.

The second group of non-public agencies must ensure that the data subject knows of the existence of data stored about him[36]. Private institutions in the third category, which process data on behalf of others, must, as a general rule, make the data subject aware of any transmittal of personal data concerning him[37]. Procedures for the exercise of access and correction rights are set out in relation to each category of data operation[38].

Variations on these patterns are to be found in the data protection laws of Austria, Belgium, Luxembourg and the Netherlands. Although it would be inaccurate to suggest that a single European model for data protection has emerged, it is nonetheless true that a number of features of the European laws distinguish them from the data protection schemes adopted in the United States. The European schemes make a greater use of licensing and other regulatory powers; they more frequently attempt to embrace both private and public institutions in their coverage; and they more frequently establish data protection authorities with broad powers to ensure the implementation and enforcement of data protection schemes.

D. ENGLAND: THE DATA PROTECTION COMMITTEE

The first major study of privacy in the United Kingdom was conducted by the Committee on Privacy (the Younger Committee), which was appointed in 1970 to consider whether legislation was needed to protect individuals and commercial and industrial interests against invasion of privacy. It was required by its terms of reference to confine its inquiries to the private sector. A survey of the use of computerized personal information systems in the public sector was undertaken by a government working party in the same year.

The Younger Committee reported in 1972 and recommended, inter alia, that the government establish an independent body to monitor "the growth in and techniques of gathering personal information and processing it with the help of computers"[39]. The committee recommended that this independent body should oversee the use of computer systems for handling personal data in both the private and the public sector.

In 1975 the government presented to Parliament the report of its internal working party on the use of computers in the public sector as a White Paper[40]. The White Paper supported the conclusion of the earlier Younger Committee report by recommending that legislation be enacted to create a permanent independent body, with powers to ensure that legal standards for safeguarding

privacy were applied to computer handling of personal information in both the public and private sectors.

A few months after the publication of the White Paper, the government appointed a Committee on Data Protection (the Lindop Committee) to advise the government on the form this permanent body should take and to consider and refine the objectives to be incorporated in legislation establishing privacy safeguards in the use of computerized personal information systems in the public and private sectors. In its 1978 report, the Lindop Committee recommended that legislation establish a Data Protection Authority (DPA) with jurisdiction over both public and private sector users of automatic personal data-handling processes[41]. The DPA would be responsible for formulating rules (codes of practice) for data users, maintaining a public register of these users, investigating complaints and ensuring compliance with the codes.

CODES OF PRACTICE

Instead of a single statutory scheme of safeguards applicable to all data users, the Lindop Committee recommended that the DPA be empowered to draft, in consultation with those affected, different codes of practice for different classes of data users[42]. These codes would be formulated in accordance with seven principles of data protection:

In the interest of data subjects

- (1) Data subjects should know what personal data relating to them are handled, why those data are needed, how they will be used, who will use them, for what purpose, and for how long;
- (2) Personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorized;
- (3) Personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used;
- (4) No more personal data should be handled than are necessary for the purposes made known or authorized;
- (5) Data subjects should be able to verify compliance with these principles;

In the interests of users

- (6) Users should be able to handle personal data in the pursuit of their lawful interest or duties to the extent and for the purposes made known or authorized without undue extra cost in money or other resources;

In the interests of the community at large

- (7) The community at large should enjoy any benefits, and be protected from any prejudice, which may flow from the handling of personal data[43].

Although these principles would be incorporated into the statute, they would not have the force of law. Instead, they would serve as guidelines for the DPA in drafting particular codes of practice. The codes would spell out specific matters, such as the kinds of data to be handled, security measures, the uses to which the data are put, their disclosure to data subjects and third parties, safeguards for ensuring accuracy, relevance, timeliness and completeness, and the circumstances in which users must seek the consent of data subjects or authorization from the DPA[44]. Thus, the rights and obligations of data subjects and data users would vary depending on which class they were assigned to by the DPA. In addition, the DPA would have authority to draft a special code of practice where a data system was considered to be unique.

The committee recommended that as appropriate codes of practice were drawn up, they should be laid before Parliament in the form of statutory instruments. If approved by Parliament, the codes would then have the force of law and their breach by a user to whom they applied would be a criminal offence[45].

REGISTRATION

To ensure that all automatic data processing systems would eventually be covered by codes of practice, the committee proposed that the legislation require all data users in central and local governments to register particulars of their information systems with the DPA. The DPA would also have the authority to call in for registration data systems used in the private sector. The DPA would maintain a register showing the particulars of each system, which code of practice applied, the date on which the data user became bound by the code, any modification of the code for the particular user, any notice served on the user by the DPA, any court order made against the user and any conviction for a data-handling offence. As a general rule this register would be

available for public inspection and copying, although the committee recommended that the DPA be given authority to place certain information (for example, information which, if disclosed, would hinder the prevention or detection of crime) on a part of the register which would be kept confidential[46].

ENFORCEMENT

The committee recommended that the DPA have a small staff of inspectors to investigate complaints and to carry out spot checks with power to order disclosure of documents and information (including official documents) and the attendance of witnesses, and to enter premises with a magistrate's warrant. The DPA would have authority to initiate criminal proceedings for a failure to comply with a requirement to register, or for breach of a code of practice[47]. In extreme cases, the court would be able to suspend the operation of a data-handling system. In addition, the committee recommended that the legislation create a civil cause of action so that a data subject who had suffered actual damage as a foreseeable result of the automatic handling of personal data in breach of a code of practice could seek compensation in the courts[48].

SPECIFIC RECORDS AND SUBJECT ACCESS

The committee did not recommend that data subjects be given a general right of access to their files in every case. It was their view that subject access should be seen as one method among others of ensuring compliance with the codes, and not as an end in itself[49]. Therefore, the committee recommended that this issue should be dealt with separately, in the various codes of practice.

However, the committee did make suggestions about subject access to specific types of records. For example, it favoured the granting of a right to social work clients to see their own computerized records as a means of ensuring the accuracy of the information in the computer[50]. Similarly, it recommended that employees be given access to their personnel records (with the possible exception of performance and salary forecasts)[51], and that parents and students be given access to school records[52]. It was the committee's view that access by patients to medical records containing judgmental data should not be prohibited, but left to the discretion of the DPA in consultation with the medical profession[53].

POLICE AND SECURITY SERVICES

The committee recommended that the handling of personal information in police computers be subject to the scrutiny of the DPA and that it be empowered to negotiate the terms of appropriate codes of practice for police records[54]. In the case of a disagreement on a major policy question between the DPA and law enforcement authorities, the committee recommended that a draft code be presented to Parliament for final decision.

With respect to criminal intelligence and national security records, the committee recommended that the DPA be empowered to play an advisory role in ensuring that the automatic processing of personal information in these areas contained appropriate privacy safeguards. The committee viewed DPA involvement as particularly important in this case since it was of the opinion that details of these systems should not become part of the public register and that there should be no right of subject access to such information[55].

THE DPA AND PUBLIC ACCOUNTABILITY

The government's White Paper, the report of the Younger Committee and the majority of witnesses who submitted briefs to the Lindop Committee all emphasized that the DPA should be independent of both private sector and government data users. On the other hand, since the DPA would be exercising a governmental function by making and enforcing regulations, it would have to be accountable to the public for its actions. The committee reconciled these two interests by recommending that the DPA be appointed by the Crown by Letters Patent[56], and report directly to Parliament.

Parliament alone would have the power to veto its codes of practice and dismiss any of its members. The committee stated that because of the potential for a conflict of interest, it would be inappropriate to make the DPA answerable to a minister[57]. In addition to direct control by Parliament of the DPA, the committee further recommended that the DPA be subject to supervision by the Parliamentary Commissioner for Administration (the English equivalent of an ombudsman), the Council on Tribunals, which oversees the adjudicative procedures of government decision-making tribunals, and the courts[58]. The committee recommended that these combined forms of supervision be used in order to ensure a full measure of accountability for the DPA in the absence of ministerial control.

E. THE UNITED STATES: FEDERAL LEGISLATION

The U.S. federal government enacted a comprehensive privacy protection scheme in the Privacy Act of 1974[59]. The act is applicable to all federal government agencies and regulates the manner in which personal record-keeping systems, both manual and computerized, are to be maintained. The intent and structure of the legislation is obviously much influenced by the report of the U.S. Department of Health, Education and Welfare[60], inasmuch as it appears designed to impose a "Code of Fair Information Practices" on each agency. The act itself states its objectives in the following terms:

The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to:

- (1) permit an individual to determine what records pertaining to him are collected, maintained, used or disseminated by such agencies;
- (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
- (3) permit an individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
- (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
- (5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemptions as has been determined by specific statutory authority; and
- (6) be subject to civil suit for any damages which occur as a result of wilful or intentional action which violates any individual's rights under this Act[61].

In brief, the provisions of the act impose certain duties with respect to the collection, storage, use and dissemination of personal data by federal government agencies, and confer certain correlative rights on individuals who are the subjects of such data. The principal rights, in terms of both the act's design and the actual enforcement of rights by data subjects, are the rights of the individual to seek access to and correction of stored data. More generally, however, any data subject who has suffered an "adverse effect" as a result of a breach of any of the statutory duties imposed on agencies may seek redress in a civil action against the agency[62]. As there is no other independent mechanism for reviewing the implementation of the act by the federal agencies, the courts, when adjudicating suits brought by data subjects, operate as the exclusive independent control over agency compliance.

The independent Privacy Protection Study Commission (PPSC) was established[63] to monitor the implementation of the act and make appropriate recommendations for its revision and, in addition, to consider the desirability of extending the application of the requirements and principles of the act to private-sector organizations. The commission published an extensive report which has proved to be a valuable resource in our deliberations[64]. In its analysis of the Privacy Act, the PPSC identified the following principles as manifested in the act's provisions:

- (1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems.
(The Openness Principle)
- (2) An individual about whom information is maintained by a record-keeping organization in individually identifiable forms shall have a right to see and copy that information.
(The Individual Access Principle)
- (3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information.
(The Individual Participation Principle)
- (4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information.
(The Collection Limitation Principle)

- (5) There shall be limits on the internal uses of information about an individual within a record-keeping organization.

(The Use Limitation Principle)

- (6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make.

(The Disclosure Limitation Principle)

- (7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate.

(The Information Management Principle)

- (8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems.

(The Accountability Principle)[65]

THE OPENNESS PRINCIPLE

The Privacy Act encourages publicity with respect to agency record-keeping practices by means of two principal devices. First, each agency is required to publish an annual notice in the Federal Register of the existence of each system of personal records it maintains. The notice must also indicate the nature of the information maintained and the agency's policies with respect to the storage, use, dissemination and disposal of the data[66]. Second, the act stipulates that when information is collected from an individual, he must be informed of the lawful authority under which the data is collected, the purpose of the collection, the uses to be made of the data, and the consequences to him if he refuses to supply the requested information[67].

Taken together, these publication requirements provide an information resource which facilitates public knowledge and scrutiny of the operation of personal data systems and an awareness on the part of the individual of the existence of data systems containing information about him and the probable uses of the data. Although the PPSC favoured continuation of these arrangements, it was critical of the quality of the information supplied by them. The commission conceded that the notices in the Federal Register are useful for allowing public scrutiny of record-keeping practices

and for internal management, but suggested that more detail is required if the notices are to "reflect more accurately the content or manner in which an agency maintains records"[68]. Similarly, the PPSC suggests that the statements made to individuals at the time of collection "are often too vague or general to inform the individual adequately"[69]. Specific suggestions for improving the quality of information communicated through each device were made in the report[70].

THE INDIVIDUAL ACCESS PRINCIPLE

The act imposes a duty on all federal agencies that maintain a "system of records" containing personal information to allow an individual about whom information is kept to review the record and obtain a copy of it in "a form comprehensible to him"[71]. In describing the nature of this right of access, two questions must be addressed: To what kinds of records does the right extend? What are the exemptions from the general principle of access?

The principal limitation on the type of record to which access is given stems from the requirement that the record be contained in a "system of records." A "record" is defined as:

...any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his name or his identifying number, symbol, or other identifying particular assigned to the individual such as a finger or voice print or a photograph[72].

In the operational sections of the Privacy Act, however, duties are imposed on agencies with respect to "systems of records." A "system of records" is defined as:

...a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual[73].
[emphasis added]

Because agencies are required to comply with the various duties imposed by the act -- including the duty to give access to the data subject -- only insofar as they maintain a system of records, any personal data not stored in a "system" is beyond the purview of the act.

The PPSC was critical of the restriction of the act's operation to record systems:

Where the Act fails to meet its objectives, the failure can often be traced, in part, to the record and system of records definition that further limits its scope of application.... Unless an agency, in fact, retrieves recorded information by reference to a "name...identifying symbol, or other identifying particular...", the system in which the information is maintained is not covered by the Act. Whereas the record definition refers to information about an individual that contains his name or identifier, the system of records definition refers to information about an individual that is retrieved by name, identifier or identifying particular. The crucial difference between the two definitions is obvious, and the effect has been to exclude many records from the Act's requirement that are not accessed by name, identifier or assigned particular[74].

The PPSC also suggested that the act is not well designed to deal with automated filing systems:

A further and extraordinarily important flaw in the system of records definition is that it springs from a manual rather than a computer-based model of information processing. In a manual record-keeping system, records are apt to be stored and retrieved by reference to a unique identifier. This, however, is not necessary in a modern computer-based system that permits attribute searches[75].

To remedy this perceived defect in the act, the PPSC proposed that data subjects be given access to any record which is "readily accessible" to the agency, whether or not it is contained in a "system of records"[76].

A second limitation on the general rule of data subject access to the record stems from sections 3(j) and 3(k) of the act, which enable agencies to exempt systems of records maintained by them from various provisions. Exemptions may be claimed under section 3(j) by the Central Intelligence Agency or by an agency which has as its principal function any activity pertaining to enforcement of the criminal law. Where the exemption is claimed, the systems of records will be exempt from all duties imposed by the act except for the requirements of annual notice and various management obligations with respect to the maintenance of the system. Exemptions under section 3(k) may be claimed by any agency if the record system consists of classified material, investigatory material compiled for law enforcement purposes, information pertaining to protective services for public

officials, statistical records, investigatory material compiled for the purpose of determining eligibility for government service or benefits (but only to the extent that disclosure of such material would reveal the identity of a confidential source), and testing or examination material. Although systems of records for which an exemption is claimed under section 3(k) are not exempt from as many duties imposed by the act as are systems exempted under section 3(j), an agency which has claimed a section 3(k) exemption is excused from granting an individual access to records concerning him, and from publishing certain information in the annual notice concerning the system.

In its study, the PPSC discovered that these exempting provisions had been relied on 6,723 times by federal agencies[77]. Again, the PPSC was of the view that this restriction on the coverage of the act was both unnecessary and inconsistent with the privacy protection objectives of the statute. Accordingly, the PPSC recommended that the device of exempting entire systems of records be abandoned and replaced by provisions which would exempt from a particular duty only certain types of records or portions of a record.

The approach to the design of exempting provisions recommended by the PPSC is similar to that adopted in the U.S. Freedom of Information Act (FOIA). As was indicated in our discussion of the FOIA in Chapter 6, the exempting provisions in that act identify particular kinds of information which are exempt from the general rule of access, and further stipulate that where exempt material is contained in a record together with non-exempt material, the latter should be segregated from the record, where possible, and disclosed to the individual who has made the request. Ironically, under current U.S. practice, an individual who wishes access to a personal record contained in a system of records which is exempt from access under sections 3(j) or 3(k) of the Privacy Act of 1974 is well advised to pursue a request for access to the record under the FOIA. Indeed, as the PPSC report indicates, this practice has been widely adopted and has resulted in the disclosure of personal information to data subjects which would not be available under the Privacy Act provisions[78].

THE INDIVIDUAL PARTICIPATION PRINCIPLE

The ability of the individual data subject to ensure the accuracy of information to which he has access under the act is facilitated by the granting of a right to seek its correction[79]. If a data subject requests an agency to correct or amend a record pertaining to himself, the agency is under a duty to either make the requested correction or to inform the data subject of its

refusal, the reasons therefor, and the right of appeal of the agency's decision. A request for amendment must be acknowledged within ten days, and a decision must be made "promptly"[80]. Where an agency does not grant the individual's request, he may file a notation of the disagreement with the agency[81]. The act further requires each agency to make rules for the implementation of these duties.

When a statement of disagreement has been filed by the data subject, the correction or disagreement must be communicated to subsequent users of the information. The information must also be communicated to third parties (outside the agency) to whom the information has been disclosed, provided that the previous disclosure is one which the agency is required to record[82].

The PPSC felt that this duty to propagate corrections was too narrowly conceived in the act. The commission recommended that a duty be imposed on an agency to forward corrections and amendments of records both to the original source of the information and to any prior recipient of the information within the agency of whom the agency would reasonably be expected to be aware, although only those previous recipients who might be expected to use the erroneous information in a decision-making process need be contacted[83].

THE COLLECTION LIMITATION PRINCIPLE

A number of devices are adopted in the act to inhibit the collection of personal data and to ensure that the procedures used in collecting data conduce to the data subject's informed decision to supply it. Thus, agencies are generally prohibited from maintaining records containing information concerning the manner in which an individual exercises First Amendment rights[84]. The act sets certain limitations on the collection and use of Social Security Numbers[85]. More generally, a duty is imposed on agencies to maintain in their records systems "only such information as is relevant and necessary" for lawful agency purposes[86]. Where the information is to be used in a decision-making process concerning the individual, agencies must use the data subject as the source of information to the greatest extent practicable[87]. Upon requesting information from the individual, the agency must inform the individual of the lawful authority for its collection, the purpose for which the information is collected, its potential uses and the consequences of refusing to supply the information[88].

In its review of the operation of these devices, the PPSC concluded that only the general duty to collect "relevant and necessary" data had effected some reduction in the amount of

personal data collected by government agencies. The broad exemptions to the provisions limiting the collection of information pertaining to the exercise of First Amendment rights and the use of Social Security Numbers enabled agencies to continue their pre-existing practices with respect to these matters. The PPSC also felt that communicating the required information to the data subject at the time of collection had not resulted in increased unwillingness on the part of data subjects to supply information[89].

THE USE LIMITATION PRINCIPLE

The act imposes limits on the extent to which personal information may be used by an agency for purposes other than the purpose for which it was supplied. Thus, unless the agency has obtained the data subject's written consent, the agency can only permit access to the record in question to "officers and employees of the agency...who have a need for the record in the performance of their duties"[90].

Although this provision obviously responds to a concern that the data subject ought not to be surprised by the uses made of information supplied by him, the PPSC concluded that the provision did not fully accomplish this privacy protection objective. Accordingly, the commission recommended that the provision be revised so as to ensure that uses of the data by agency personnel would be compatible with the purpose for which the information was collected, and consistent with the reasonable expectations of the data subject with respect to the use of the data by the agency[91].

THE DISCLOSURE LIMITATION PRINCIPLE

The act adopts as a general principle the proposition that federal agencies should not disclose personal information to outsiders unless the disclosure fits within one of ten categories of permitted disclosure. The most important of these exceptional categories permits disclosure for a "routine use," that is to say, "for a purpose which is compatible with the purpose for which [the record] was collected"[92]. The other exceptions permit disclosures to agencies for civil or criminal law enforcement, to the National Archives, to either House of Congress, to the Comptroller General, to a recipient who proposes to use the information solely for research or statistical purposes, to an individual in circumstances affecting health or safety, and pursuant to requests for access made under the U.S. Freedom of Information Act where

disclosure does not constitute a "clearly unwarranted invasion of privacy"[93].

The concept of "routine use" was the major concern addressed by the PPSC with respect to the operation of this provision. The commission found that federal agencies had adopted the practice of construing very broadly the range of permitted disclosures. Accordingly, the commission recommended that the act's definition of "routine use" be revised to permit disclosures only where the disclosure is both compatible with the purpose for which the information was collected and consistent with the reasonable expectations concerning disclosure under which the information was initially obtained[94].

A further difficulty involved the exemption for disclosures pursuant to Freedom of Information Act (FOIA) requests. The PPSC was of the view that agency personnel exhibited some difficulty in applying the FOIA standard of a "clearly unwarranted invasion of privacy," and recommended the establishment of an independent federal agency which would issue interpretative rules indicating more clearly situations in which disclosure of personal information to third parties would be permissible[95].

THE INFORMATION MANAGEMENT PRINCIPLE

Federal agencies are obliged under the act to adopt policies and practices of information management conducive to accuracy in record keeping and the security of confidential personal information. The act stipulates that agencies must "maintain all records which are used by the agency in making any determination about an individual with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination"[96]. Further, the act requires each agency to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom the information is maintained"[97].

The PPSC expressed two concerns with respect to the operation of these provisions. First, the commission concluded that the accuracy of agency record-keeping practices suffered from the absence of an obligation to propagate corrections to personal records throughout its own systems. As noted previously, the act imposes obligations on agencies only to forward corrections to all subsequent users of the information and previous recipients of the data who are not employees of the agency. The PPSC was of the

view that the failure to propagate corrections throughout the agency's record-keeping systems resulted in decisions made on the basis of inaccurate information. Accordingly, the commission recommended that agencies be required to propagate or forward corrections to previous recipients of the information within the agency itself in situations where it could reasonably be expected that the corrected information might be used in a decision-making process[98].

Second, the commission expressed concern that in a number of federal agencies, there was an absence of effective implementation of the provisions of the act. The commission noted that those agencies which had established an internal formal mechanism to oversee implementation were the most successful in this regard. Accordingly, the commission made the following recommendation:

In order to provide for more effective implementation of the Act, the Commission believes that the head of each agency should designate one official with authority to oversee implementation of the Act. The official's responsibilities would include issuing instructions, guidelines, and standards, and making such determinations, as are necessary for the implementation of the Act. He would also be responsible for taking reasonable affirmative steps to assure that all agency employees and officials responsible for the collection, maintenance, use and dissemination of individually identifiable records are aware of the requirements of the Act[99].

THE ACCOUNTABILITY PRINCIPLE

Many of the provisions of the act are designed with the apparent objective of ensuring that federal agencies be accountable for their personal record-keeping practices and, in particular, that they adhere to the principles underlying the act. The provisions requiring the publication of annual notices and permitting data subjects to have access to their files contribute to some measure of accountability. In addition, the act stipulates that agencies must maintain an accounting of disclosures of personal information to third parties. The accounting of disclosures is to be made available to data subjects seeking access to their records, thus providing an additional mechanism for the monitoring of agency activity by the data subject[100].

The act requires that the accounting indicate the date, nature and purpose of the disclosure and the identity of the recipient; no accounting is required for "routine use" or disclosures under the Freedom of Information Act[101]. The data

subject may inspect the accounting, which is retained by the agency for five years or the life of the record, whichever is longer[102]. Agencies are not required, however, to disclose accountings relating to transfers for law enforcement purposes[103].

Apart from permitting the data subject to monitor the nature and extent of agency disclosures of personal information pertaining to him, the accounting requirement is also important in facilitating the propagation of corrections by the agency to third parties to whom the erroneous information has previously been communicated. Agencies are required by the act to inform any prior recipient of whom they have maintained an accounting of corrections made to the record[104].

The accounting requirement has imposed substantial administrative burdens on federal agencies. Nonetheless, the PPSC felt that it should be retained in a modified form. It was the commission's view that the primary purpose of the requirement was to facilitate the propagation of corrections. Accordingly, it was recommended that the accounting be maintained in such a way as to parallel the recommended revisions to the statutory duty to propagate corrections: an accounting should be maintained with respect to disclosures within the agency as well as those to third parties. In extending the duty to cover disclosures within the agency, of course, the commission was adding to the burden imposed by the provision. With respect to disclosures to third parties, however, the accounting burden would be reduced inasmuch as the duty would extend only to disclosures to third parties to whom the agency would be required, under the revised act, to propagate corrections. (Essentially these are any third parties who may reasonably be expected to use the information in a decision-making process, or any sources of information who would not otherwise be expected to become aware of the error in question[105].)

The act provides an additional means of accountability through the creation of rights of redress in the civil courts for data subjects who have been adversely affected by agency practices contravening the provisions of the act[106]. The PPSC expressed the opinion that, apart from cases in which individuals seek judicial review of denials of access or correction rights, the operation of the civil remedy as an accountability mechanism is insignificant. Accordingly, the commission made two recommendations aimed at making the civil remedy a more effective avenue of redress for individual data subjects: first, the act's requirement that the individual must show an "adverse effect" resulting from an agency practice should be abandoned. The demonstration of such an adverse effect might be very difficult in many cases. The elimination of this requirement would make it easier for data

subjects to come forward and seek judicial review of unlawful agency practices. Second, the commission recommended that the act be revised to permit the recovery of monetary compensation, or "general damages," for intangible interests such as pain and suffering, loss of reputation, or the chilling effect on constitutional rights resulting from excessive collection of data. It was the commission's view that the present act's limitation of recovery to "actual damages" might operate as a disincentive for the bringing of meritorious claims in which no measurable pecuniary loss has been suffered by the data subject whose privacy interests have been undermined by agency record-keeping practices[107].

Although the PPSC concluded that improvements could be made to the act's provisions relating to civil liability, the commission also felt that the act was fundamentally flawed insofar as it relied exclusively on the initiative of data subjects in seeking effective review of agency practices:

Someone other than the individual record subject must be in a position to hold agency record-keepers accountable; the Act's individual enforcement model is simply ineffective on a broad scale[108].

Moreover, the commission was not persuaded that the criminal penalties imposed under the statute provided an effective substitute for the establishment of a means of more direct supervision of agency practices.

The criminal penalties established by the Privacy Act deal with three matters. First, wrongful disclosure by agency employees of records about individuals is constituted an offence if the disclosure is made "wilfully" by an employee who knows that disclosure is prohibited by the act[109]. Second, failure to comply with the system notice requirements of the act is also an offence for agency employees[110]. For these two offences, the officer or employee of the agency may be personally liable to pay the fine imposed. The third offence created by the act prohibits the requesting of a file by any person under false pretenses[111]. In the case of each offence, a maximum fine of \$5,000 may be imposed.

The PPSC suggests that in the absence of effective supervision of the implementation of the act, the offence provisions have proved to be something of a mixed blessing. The existence of criminal penalties for wrongful disclosure of data is widely known among agency personnel, and, in the commission's view, "too often" results in denials of access[112].

In summary, then, the U.S. Privacy Act of 1974 establishes a comprehensive scheme of data protection applicable to personal record keeping by federal government agencies. The U.S. statute differs from many European schemes by failing to provide for the establishment of an independent authority to oversee the implementation of the privacy protection principles established in the act. The individual data subject provides the exclusive initiative for independent review of agency compliance with the act.

The Privacy Protection Study Commission, in its detailed study of the operation of the act, made a number of suggestions for its revision and improvement. In particular, the commission recommended that the operational sections of the act should not be triggered by the concept of "systems of records." Subject access and correction rights and the exemptions from the applicability of the statutory duties imposed by the act should be applicable, in principle, to all record systems. Additional suggestions were made by the commission for the purpose of strengthening the rules relating to internal agency use of personal information and disclosure of information to third parties. Finally, the commission expressed some concern about the effectiveness of the implementation mechanisms set forth in the statute and made a number of suggestions for their improvement.

COSTS OF IMPLEMENTING THE PRIVACY ACT OF 1974

The PPSC made an attempt to ascertain the approximate cost of implementing the provisions of the Privacy Act throughout the agencies of the federal government[113]. It would appear that the costs of implementation are substantially less than was first estimated. The Office of Management and Budget (OMB) had estimated in 1974 that implementing the act would cost \$200-\$300 million per year over the first four to five years, and would require an additional start-up cost in the first two years of operation of \$100 million. In fact, however, the actual costs proved to be much less than these estimates. In 1977, the OMB estimated that start-up costs in the first nine months between the date of its passage and the date it became effective were \$29,459,000, and that first year operating expenses were an additional \$36,599,000. A breakdown of these amounts into various categories of expenditure is shown in Figure 1.

Six large federal agencies (the Departments of Treasury, Defense, Justice, and Health, Education and Welfare, the Veteran's Administration and the CIA) accounted for 93 per cent of the expenditures. The Department of Defense alone accounted for 48 per cent.

Figure 1

Cost of Implementing the Privacy Act of 1974

Summary - All agencies
(Outlays in Thousands of Dollars)

	Start Up ¹		Operations ²	
Publication Requirements	\$13,549	46.0%	\$ 4,405	12.0%
Training	6,825	23.2	3,282	9.0
Granting Access	914	3.1	10,670	29.2
Correcting Records	483	1.6	2,116	5.8
Security and Control	2,175	7.4	1,345	3.7
Accounting for Disclosures	667	2.3	9,415	25.7
New Data Collection Procedures	1,164	4.0	1,507	4.1
All Other Costs	3,728	12.7	4,012	11.0
Reductions from Records/Systems Eliminated	-45	-0.2	-62	-0.2
Collections	- 2		-91	-0.2
Total ³	\$29,459	100.0%	\$36,599	100.0%

¹ Start up costs include any one-time costs incurred from January 1, 1975 through September 30, 1976.

² Operating costs cover the period September 27, 1975 through September 30, 1976.

³ Totals may not add due to rounding.

Source: Federal Personal Data Systems Subject to the Privacy Act of 1974, Second Annual Report of the President, Calendar Year 1976, p.23.

From the PPSC Report, Appendix 4, 40.

F. U.S. STATE LEGISLATION

Many state governments in the United States have enacted privacy protective legislation regulating the use of specific types of records containing personal information about individuals. Forty-eight states regulate medical records; thirty-two states regulate school records; twenty-seven regulate tax records; and twenty-seven regulate arrest records. Twenty-one states regulate criminal justice records in general, and a total of thirty-four states regulate some form of criminal justice records. Nineteen states regulate credit records, and legislation is pending in one state. Other types of records regulated to lesser degrees are bank records (six states); data banks (four states); and employment records (four states). Use of the Social Security Number is regulated by five states. It should also be noted that privacy as a right is protected by state constitution and by common law in the majority of states[114].

Of more interest in the present context, nine states have enacted comprehensive privacy legislation or Fair Information Practices Acts: Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, Ohio, Utah and Virginia[115]. (Several other states have considered but have not yet enacted such legislation.) Generally, all of these statutes, which primarily govern the public sector, follow the guidelines of the 1973 Health, Education and Welfare Report. They are similar in many respects to the general scheme adopted in the U.S. Privacy Act of 1974.

The statutes impose information management duties on government agencies similar to those in the Privacy Act and confer on data subjects broad rights of access to and correction of records. Civil and criminal liabilities are typically imposed for certain breaches of fair information practices. Like the federal statute, these schemes apply both to computerized and to manually-stored personal information systems.

In view of the general similarity of the state legislation to the federal act, it will not be useful to offer an exhaustive account of each state's privacy protection scheme. Nevertheless, it may be helpful to discuss three features of these state laws not found in the federal statute: first, provisions extending coverage to local governmental institutions; second, the adoption of data classification schemes; third, the establishment of independent privacy boards or agencies to supervise implementation of the legislation.

INSTITUTIONAL COVERAGE

Four of the nine statutes (those of California, Connecticut, Indiana, and Utah) apply to state-administered agencies only. The other five statutes are more sweeping in their coverage. The statutes of Massachusetts, Minnesota, and Virginia are the most far-reaching, requiring both state level and local governmental institutions, and even some quasi-public and private entities, to comply with the statute. The Ohio and Arkansas statutes fall between the two extremes, applying to state and local governmental agencies, but not to private corporations.

DATA CLASSIFICATION SCHEMES

Four states (California, Indiana, Minnesota and Utah) have developed schemes for classifying data in various categories, with different confidentiality and disclosure rules for each category.

Section 1 of the California Information Practices Bill classifies personal data in the following three categories:

- a. personal information, the dissemination of which and the accessibility of which is, to some extent, controlled by the individual;
- b. confidential information, which is usually inaccessible to the subject and controlled primarily by the agency;
- c. non-personal information, which is considered neutral and accessible to anyone in the private or public arena.

Section 1 of the Indiana Fair Information Practices Act employs a more complicated classification system, dividing data into four categories. The first three (private, confidential and unrestricted) are similar to the categories in the California legislation. The additional category, restricted, refers to "private information for which the data subject has given consent for limited disclosure or for which such consent has not been given but for which a compelling public interest in public disclosure may arise."

Minnesota and Utah, the first states to pass such legislation, use three classifications of data in their privacy statutes (private, confidential and public). Under section 1 of the Minnesota law, private data is that "which is not public but which by law is accessible to the individual subject of the data." Confidential data is that which "is not public but is (a) expressly

made confidential by law as to the individual subject of that data; (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action, is upon the agency." Public data is that "which is accessible to the public in accordance with the provisions of section 15.17 [a freedom of information law]."

The other statutes adopt the more common device of making the provisions of the act broadly applicable to all personal data and then exempting certain kinds of data from the fair information practices established in the statute. In the Massachusetts act, section 1 defines personal data as "any information concerning an individual which, because of name, identifying number, mark or description, can be readily associated with a particular individual." The Arkansas act adds the phrase "finger or voiceprint or picture, and including any combination of such characters" to its definition[116]. Section 1(D) of the Ohio act defines "personal information" more broadly as "any information that describes anything about a person, or indicates actions done by or to a person, or indicates that a person possesses certain personal characteristics, and that contains a name, identifying number, symbol, or other identifier assigned to a person." The Connecticut and Virginia acts specifically refer to types of information which may be considered personal, such as "any information about a person's education, finances, medical or emotional condition or history, criminal history, employment or business history, family or personal relationships, reputation or character"[117], or "all information that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics...and the record of his presence, registration, or membership in an organization or activity, or admission to an institution"[118].

The data classification technique at first appears to offer the promise of greater certainty in the identification of rights and obligations pertaining to certain kinds of personal data. In particular, it appears to offer a more straightforward solution to the problem of determining when personal privacy should be invaded for the purpose of granting access to personal information to the public under the banner of "freedom of information." The usual device employed in U.S. freedom of information and privacy laws is to permit disclosure when it will not constitute a "clearly unwarranted invasion of privacy" -- a test which is, at best, rather too vague and general to offer clear guidance to the public servants and courts who must apply it.

On closer examination, however, the promise of greater certainty appears to be largely illusory. The use of a data classification scheme is a matter of drafting style rather than of substantive policy. Thus, "confidential information" is defined in the California statute in a manner which parallels the typical exemptions from the subject access rules in other statutes. The ultimate effect is indistinguishable from that of the more common drafting style. An illustration may clarify the point. Under privacy statutes which do not use a classification scheme, data subjects are, for example, usually denied rights of access to certain kinds of law enforcement information. Under the California act, data subjects are generally denied access to "confidential information"[119]. Confidential information is, in turn, defined in the act to include law enforcement information[120]. Moreover, with respect to the question of disclosure of personal information to members of the public, the California act permits disclosure of any personal data, including "confidential information" if it is accessible to the public under the California freedom of information law[121]. Thus, one is ultimately required to determine whether, under that statute, the disclosure of the particular information in question would constitute a "clearly unwarranted invasion of privacy"[122]. In short, the use of classification schemes does not appear to effect a marked change from or improvement upon the more common drafting techniques.

THE ESTABLISHMENT OF INFORMATION PRACTICES BOARDS

A common feature of the state privacy schemes is the establishment of an agency or commission -- often called an Information Practices Board -- whose mandate it is to oversee the implementation of the scheme by governmental agencies and assist in the resolution of disputes with data subjects.

Under the California act, for example, an Office of Information Practices has the power to develop guidelines to assist government bodies in the implementation of the privacy protection scheme. The office is to assist governmental agencies in "meeting technical and administrative requirements"[123], and may establish regulations prescribing the form and method of the annual notices required by the act for each data system[124].

As well, the office provides educational and dispute resolution facilities to record subjects and other interested citizens. It must set up a toll-free telephone line for citizens seeking aid, and must help requesting individuals identify records about themselves and secure access to those records[125]. Upon receiving a complaint from any citizen about any matter covered by

the act, the office "may investigate, determine, and report any violation of any provision of this chapter, or any regulation adopted pursuant thereto..."[126], and "may attempt to mediate any dispute between the agency and a complaining individual.... In the event that mediation fails, the Office of Information Practices shall issue a statement of its findings and recommendations to the parties..."[127]. Further, the office "shall report on violations of this chapter, of which it has knowledge, to the affected agency and if the violation is not corrected within 60 days, to the Office of the Governor, the Legislature and the appropriate law enforcement agency"[128]. In addition to these procedures, the Office of Information Practices, the Attorney General, any district attorney, an individual acting on his own behalf, or any member of the public may seek a court order enjoining an agency from engaging in improper practices[129].

The Minnesota statute delegates privacy protection responsibilities to two agencies, one of which promulgates regulations for the purpose of implementing the statutory scheme, and one of which engages in ongoing research and study of privacy-related problems. The regulatory authority is conferred on the Commissioner of the Department of Administration. The commissioner is required to promulgate rules implementing the statutory scheme, in accordance with standard rule-making procedures in the Minnesota Administrative Procedures Act. Prior to adoption of these rules, the commissioner is required to give notice to all affected state agencies and political subdivisions, and conduct public hearings. The rules must not, however, affect the rights of data subjects conferred by the act. Apart from promulgating rules, the main responsibility of the commissioner consists in preparing an annual report to the legislature summarizing the information contained in the annual data systems notices required by the act, and notifying the legislature of any problems relating to the administration, implementation and enforcement of any of the sections of the act, especially those which might, in his opinion, require legislative action[130]. The research function is performed by the Privacy Study Commission, a body established by the act, which consists of six members, three of whom are appointed by a legislative committee and three of whom are appointed by the Speaker of the House. The commission's primary responsibility is to make a "continuing study and investigation of data on individuals collected, stored, used and disseminated by political subdivisions, state agencies, statewide systems, and any other public or private entity in the state of Minnesota the commission may deem appropriate for such study and investigation"[131]. (It is our understanding that the large volume of research work necessarily associated with the use of personal data by public institutions has thus far prevented the commission from examining private sector privacy problems.) The commission is granted extensive investigatory powers to enable it

to carry out its mandate. The commission may issue subpoenas "requiring the appearance of persons, production of relevant records, and the giving of relevant testimony"[132]. Ultimately its research work is expected to lead to recommendations for legislative action, administrative action or voluntary adoption of whatever requirements and principles are deemed necessary "to protect the privacy of individuals while meeting the legitimate needs of government and society for information"[133].

Variations on these institutional patterns are to be found in the privacy acts of Arkansas, Indiana, Ohio and Utah. The Connecticut, Massachusetts and Virginia statutes do not establish similar administrative supervisory and enforcement mechanisms. All nine of the state laws do provide, however, for some form of judicial review of agency conduct through court adjudication of disputes between data subjects and governmental agencies.

G. CANADA: THE CANADIAN HUMAN RIGHTS ACT, PART IV

The purpose of Part IV of the Canadian Human Rights Act[134] is to guarantee to individuals rights of access and correction with respect to personal information about them held by federal government departments and institutions, and to control the use and dissemination of this information[135].

The central features of the legislation are as follows. First, the act requires the publication of an annual index describing all "federal information banks"[136] which are defined, in effect, as stores of personal information maintained by the Canadian government for use in decision-making processes. Second, the act sets out a statement of rights of subject access to and correction of this data[137]. Third, the act permits record keepers to transfer data for administrative purposes only if the proposed use is "derivative" (consistent with the use for which the data was first collected) or if the data subject has consented to the transfer[138]. Fourth, the act provides that complaints about violation of data subject rights conferred by the act are to be investigated by the Privacy Commissioner[139]. Finally, the act gives authority to the Treasury Board (the federal government agency primarily responsible for financial administration) to oversee future collection and storage of personal information[140]. In exercising its responsibilities under the act, the Treasury Board has developed an elaborate set of directives and guidelines which are evidently designed to ensure implementation of the privacy protection objectives of the act[141]. These directives and guidelines are not promulgated under the act as regulations and hence do not have the force of law. However, the Treasury Board has indicated that directives are to be adhered to

unless a deviation has been consented to by the Treasury Board. Guidelines are not mandatory but "should be followed unless there is good reason not to do so." In the outline which follows, describing the ways in which the federal scheme deals with collection of data, subject access and correction rights, transfers of data, and administration and enforcement mechanisms, we will refer to the provisions of the act and the regulations promulgated thereunder, as well as to these Treasury Board directives and guidelines.

COLLECTION OF INFORMATION

The act itself places no limits on the types of personal information to be gathered from record subjects, nor does it set up any code or rules defining agency obligations and subject rights during the collection process. However, section 56(2) authorizes the "designated minister" (in this case, the President of the Treasury Board) to review and make recommendations about these activities.

In order to coordinate the collection of information for... information banks within the control of government institutions and to eliminate wherever possible any unnecessary collection of information for storage in such information banks, the designated Minister shall cause to be kept under review the utilization of existing information banks and proposals for the creation of new information banks or the substantial modification of existing ones and shall make such recommendations as he considers appropriate to appropriate Ministers with regard to information banks that, in his opinion, are underutilized or the existence of which can be terminated.

The act also recognizes the importance of regulating collection activities at the systems-design stage; it directs that no new information bank shall be established and that no substantial modification of existing banks shall be made without the approval of the Treasury Board[142]. In addition, section 62(3) deals with the collection process by granting the Governor in Council powers to make regulations

- (b) prescribing any special procedures to be followed by a government institution in obtaining personal information for inclusion in a federal information bank;

and

- (g) providing for the management and surveillance of records of any government institution to promote the protection of individual privacy and to ensure that the provisions of this Part are complied with.

The regulations[143] promulgated in the exercise of this authority provide, in effect, that

no personal information may be collected in a federal information bank unless the bank has been duly registered by the Treasury Board;

wherever possible, government institutions shall collect personal information directly from the record subject; and

government institutions shall inform the record subject of "the purposes to be served by such collection, the authority therefor and the rights of the individual under the Act."

The Treasury Board directives and guidelines which implement the policy of the act and the regulations with respect to collection show a concern to reduce, where possible, the collection of personal data. In an introductory statement, it is suggested that "government institutions may not collect irrelevant, unjustified or intensely discriminatory information"[144]. A mandatory directive provides as follows:

Government institutions shall maintain only those banks of information (BIN) for which:

- (a) information can be directly related to the authority under which it operates or to approved program and activity objectives;
- (b) the benefit to be derived from the use of the information outweighs the cost to the government institution and the response burden placed on data sources;
- (c) the use of information in the BIN cannot result in a discriminatory practice based on proscribed grounds of discrimination set out in Part I of the Canadian Human Rights Act[145].

A further objective set forth in the guidelines which may have the effect of reducing the collection of personal data is embodied in the Treasury Board's directive that banks of information (BINs) "shall be designed to minimize the response burden"[146]. Among the techniques suggested by the board for

lessening the response burden imposed on data subjects is "reducing the number of questions" and "reducing frequency of collection"[147].

Other aspects of the methodology for reducing the response burden may appear to be less clearly conducive to privacy protection. For example, it is suggested that response burden can be minimized by "using existing information rather than establishing new BINs"[148]. The board also sets forth a mandatory directive that "government institutions shall design the collection of information for inclusion in BINs to meet as many federal government uses as possible..."[149]. The establishment of such multi-use personal data banks may be inconsistent with a general policy of attempting to ensure that personal information submitted for one purpose will not be used for another. Nonetheless, two limiting factors in the board's policies may lessen the risk of such use. First, the data subject is, as a general rule, to be informed of the uses to which personal information will be put. Second, the board's policies on collection are subject to the general rule that data collected for one administrative purpose cannot be used for another unless the data subject has consented to the further use or unless the further use is "derivative."

The Treasury Board guidelines also deal with implementation of the regulations relating to the manner in which data are collected (for example, the rules that personal data should, where possible, be collected directly from the data subject, and that the subject should be informed of the purposes to be served by the collection as well as his rights under the act). In addition, the board has published a mandatory directive which states that "in the course of collecting information for inclusion in a BIN, data sources shall not be given the impression that response is mandatory unless response is legally required"[150].

SUBJECT ACCESS AND CORRECTION RIGHTS

Under the act, a data subject is entitled to obtain access only to those records in the control of the governmental institution which identify him by name or otherwise allow "readily ascertainable" identification, and are used by the institution in a decision-making process relating directly to him. Section 52(1) of the act entitles an individual to

1. examine the record;
2. know how the record has been used since its creation, or since the act came into force;

3. request corrections;
4. require that a notation of a requested correction be made on the record, if the record is not amended in accordance with his request.

The act itself is silent about the procedures for granting subject access. However, the Treasury Board's Administrative Policy Manual outlines methods for verifying an applicant's identity, for making the record available if a copy is not requested, and for determining what kinds of data are available[151].

Acknowledgement of correction requests must be made within thirty days. Different criteria are set for processing requests for changes to factual material and opinion data. In the latter case, it appears that a correction request will result in a notation of the data subject's differing opinion on the files.

Access to government-held records is facilitated by the statutory requirement that the Treasury Board publish an annual index of federal information banks, which must contain the names of all government data banks and describe the kinds of records they contain[152]. Each data bank listing includes the name of a person to consult when requesting access to a record.

The act permits Cabinet ministers to exempt either an entire information bank or a particular record or portions thereof from the general requirements of publication and subject access. For example, where a minister is of the opinion that disclosure of the existence of the information bank or of the information it contains would be injurious to international relations, national defence or security, or federal-provincial relations, or would be likely to disclose information collected by an investigatory branch of government, or would be detrimental to the operation of the prison system, he may, with the approval of the Cabinet, order that the information to be published about it in the index be restricted and that subject access be denied[153].

Similarly, the appropriate minister has discretion to deny subject access to particular records or portions thereof if he is of the opinion that knowledge of the existence of the record or of information contained in it would be harmful to any of the interests outlined above; if it might reveal personal information about another individual; if it might impede the operation of a court of law or other tribunal; or if it might disclose legal advice given to the government[154]. The appropriate minister may also order that subject access to a record be denied if, in his opinion, the public benefit to be derived from permitting subject access to such records is outweighed by the costs of providing access[155].

Thus, the statutory exemptions from the publication and subject access requirements of Part IV give broad discretion to ministers to override the provisions of the act. However, in most cases, the mandatory Treasury Board directives outlining the procedures to be followed require consultation with other officials or ministers prior to claiming an exemption from the act.

Finally, it should be noted that although section 52(1) of the act entitles the individual to "know how the record has been used since its creation," there is no requirement, statutory or otherwise, that a record of disclosures of the file be maintained. The individual data subject presumably is apprised of the uses made of the information either by being informed of its potential uses at the time of collection or, where the statute so requires, when the consent of the data subject for a proposed transfer is needed.

TRANSFER OF RECORDS

In common with many other North American privacy protection schemes, the act sets forth a general rule that no transfer of records can be made unless certain conditions are met. This limitation on transfers is achieved primarily through the concepts of "derivative" and "non-derivative" uses of records; a derivative use is a use "consistent with the use for which [the record] was compiled"[156]. The index published by the Treasury Board must contain a description of derivative uses. In order to make other administrative use of a record a government institution must seek the consent of the individual. Section 52(2) provides as follows:

Every individual is entitled to be consulted and must consent before personal information concerning that individual that was provided by that individual to a government institution for a particular purpose is used or made available for use for any non-derivative use for an administrative purpose unless the use of that information for that non-derivative use is authorized by or pursuant to law [emphasis added].

The essential character of the provision rests on a decision that the no-transfer rule ought to be precisely aimed at the problem of administrative use of personal information for a purpose other than that for which it was collected. For example, medical information supplied for the purpose of gaining veterans' benefits should not be used in the making of a decision not to employ the veteran in question in the public service.

While the notion of "derivative use" is similar to the U.S. Privacy Act concept of "routine use" (derivative use requires "consistency" with the original purpose for collection; routine use is defined in terms of "compatibility" with the original purpose), the Canadian Human Rights Act provision develops a much more modest no-transfer rule than does the Privacy Act in the United States. First, the Canadian Human Rights Act no-transfer rule applies only to data submitted by the data subject. Information collected from third-party sources (such as friends, neighbours, or private sector institutions) or, indeed, generated by government itself, is not covered by the rule. Second, the rule only prohibits transfers for an "administrative purpose" which is not a derivative use. The section does not regulate transfers for other purposes. In theory, then, the federal government could disclose identifiable individual data to any person or institution, provided that the recipient does not propose to use the information for an "administrative purpose." ("Administrative purpose" is defined in section 49 of the act as "the use of [a] record in a decision-making process that relates directly to that individual.") Where an agency wishes to use information supplied for one administrative purpose for another such purpose, it may do so as long as the second administrative use is "consistent" with the purpose for which it was originally submitted by the data subject. (For example, information supplied by an individual on a licence application form might be used by the licensing agency in the context of a later decision to revoke the licence granted pursuant to the original application.) The U.S. Privacy Act, on the other hand, regulates all transfers of identifiable data by providing that no agency shall disclose "any record" unless one of the eleven exempting provisions applies.

There is, of course, one fundamental distinction between the Canadian and U.S. schemes. In the Canadian act, the derivative use is one which is determined to be such by the minister, while under the U.S. Act, the standard is not (in theory at least) subject to interpretation at the discretion of the agency. It is difficult to gain a clear understanding of how the Canadian no-transfer rule is to operate without some appreciation of how ministerial discretion with respect to the "derivative use" concept is deployed. The Treasury Board has developed an elaborate set of guidelines relating to the proper interpretation of "derivative use." Since the various departments and agencies covered by the Canadian Human Rights Act are likely to adhere fairly closely to these guidelines, they give some indication of how the concept of derivative use works in practice. The Treasury Board's interpretation of the derivative use concept is as follows:

Consistency with the particular purpose

A derivative use is one that is consistent with the particular purpose. The most important category of derivative use is the use, by the collecting agency, that has an obvious relationship with the particular purpose. For example, the particular purpose of information provided by an applicant for some benefit would be the decision to grant the benefit. Derivative use would include statistical research by the agency concerned with the effectiveness of the benefit program, uses in conjunction with a similar benefit program operated by the agency, and uses in conjunction with auditing and policing the benefit. More generally, a use should be generally claimed as derivative (a) if it is connected with the main work of the agency that collected this information; or (b) if it is used by other agencies in an application connected with the particular purpose, provided that the individual who supplied the information was aware of, or could have reasonably inferred such use at the time of collection. On the other hand, a use should be generally claimed as non-derivative if it results in information going to another agency for purposes not directly connected with the operation of the program for which the information was collected or if the use within the agency is sufficiently novel that the individual could not reasonably have anticipated uses of this type at the time of collection.

An exception relates to information supplied under legal compulsion or to obtain financial benefit. In these cases, derivative use should be defined narrowly to correspond closely to the particular purpose, to uses in obtaining closely associated benefits, or to policing and auditing of these benefits [emphasis added] [157].

This view of derivative use is rather similar to the refined concept of "routine use" recommended by the PPSC in its review of the operation of the Privacy Act. The underlined portion above contains language which is remarkably similar to the revised definition of routine use proposed by the PPSC. Although the Canadian Human Rights Act no-transfer rule controls a much narrower range of transfers than does the U.S. Privacy Act, the Treasury Board elaboration does present a fairly restrictive notion of the concept of routine information transfers.

The matter of informed and voluntary consent is also regulated to some extent in the Treasury Board guidelines. In brief, the guidelines require that when consent is sought, the non-derivative use should be precisely identified, the data subject should be given an opportunity to positively indicate his

consent, and he should be advised that any refusal to consent for non-derivative use will not result in an adverse decision in conjunction with the particular purpose being served by the collection of information[158]. Although the agency is permitted to seek consent either at the time of collection or subsequently, some attempt is made to control the format of the request for consent in order to ensure that it is informed and voluntary. The final problem identified by the U.S. PPSC (access by legislators making interventions on behalf of their constituents) is dealt with by the Treasury Board guidelines on the basis that such use would be derivative and, accordingly, access may be given.

ADMINISTRATION AND ENFORCEMENT

The President of the Treasury Board is responsible for the administration of the act and for ensuring that governmental institutions operate their information banks in accordance with directives and guidelines issued by the board. Substantial changes to existing systems or the creation of new information banks are subject to the board's approval. The use and possible termination of existing data banks are matters on which the board may conduct investigations and make recommendations to the appropriate minister.

The act also establishes the office of the Privacy Commissioner, who is a full-time member of the Canadian Human Rights Commission appointed by the Minister of Justice[159]. The Privacy Commissioner is responsible for ensuring that the rights provided by Part IV are extended to the public by the government departments and agencies covered by the statute. Individuals who allege that their Part IV rights have been violated have the right to complain to the Privacy Commissioner, who must investigate all complaints[160]. If the commissioner finds that the rights of a data subject have been violated or denied, he reports his findings to the minister responsible for the government agency concerned[161]. However, the commissioner's powers are limited to making recommendations for action: he cannot compel an agency to change its record-keeping practices or initiate court proceedings for breach of the statute. In fact, the statute does not provide civil or criminal liability for breaches of the rights it creates. Individuals whose rights are infringed must rely on the Privacy Commissioner's ability to negotiate for redress with the governmental institution in question. To allow parliamentary and public scrutiny of the operations of the Office of the Privacy Commissioner, the act requires that the commissioner file an annual report with the Minister of Justice, who must lay it before Parliament[162].

The Canadian act differs from most European legislation and from the data protection scheme recommended by the British Lindop Committee in that there is no independent authority with the power to compel government data users to comply with the principles of the statute. Responsibility for administration and general supervision lies with the Treasury Board, which is part of the existing administrative machinery of government and whose mandate embraces much more than privacy protection. Responsibility for ensuring that data subjects' rights are protected lies with the Privacy Commissioner, whose powers are advisory only.

H. CANADA: PROVINCIAL PRIVACY LEGISLATION

Although there are no provincial statutes similar in nature to Part IV of the federal Canadian Human Rights Act ensuring the protection of personal privacy in the context of government data-handling practices[163], three provinces have enacted general statutes making invasion of privacy a ground for a civil suit by the person affected. Anglo-Canadian common law does not explicitly recognize a right to privacy; the Manitoba, Saskatchewan and British Columbia privacy acts attempt to remedy this perceived deficiency by creating a statutory cause of action for privacy invasion[164].

None of the three acts requires the complainant to show financial loss in order to succeed: the invasion or violation of privacy is itself deemed to be sufficient injury to merit compensation. The right to privacy is defined differently in the acts. In British Columbia, for example, the "nature and degree" of privacy to which an individual is entitled is limited to what is "reasonable in the circumstances"[165]. Other sections of the acts suggest that their primary intent is to control unwarranted invasions of physical privacy by way of eavesdropping, surveillance and the unauthorized use of another's likeness for profit.

The Manitoba and Saskatchewan acts provide that the unauthorized use of letters, diaries and other personal documents may constitute an invasion of privacy[166]. These two statutes recognize to some extent the concept of informational privacy, which is the primary concern of this Commission. However, none of the three privacy acts deals expressly with the inappropriate or unauthorized use of personal information which has been given voluntarily to another person or institution and integrated in an information bank.

By explicitly recognizing personal privacy as an interest worthy of legal protection in its own right, these statutes are an advance from the position of Anglo-Canadian common law, and under

certain circumstances they may provide redress for wrongful invasions of privacy[167]. However, they are basically reforms of existing tort law, and do not fully address the problems of data-handling practices in the computer age. The usefulness of tort law in protecting informational privacy will be discussed in more detail in the next chapter.

I. NEW SOUTH WALES: THE PRIVACY COMMITTEE

It is of interest to compare the data protection schemes developed in Europe and North America to the rather different approach adopted by New South Wales, Australia, in dealing with privacy protection problems. The New South Wales Privacy Committee was established by legislation in 1975[168]. Essentially, the powers of the committee are to engage in research and investigation of privacy protection problems, broadly construed, and to seek the resolution of specific complaints brought to the committee's attention by individuals who feel that their privacy has been invaded[169].

The general structure and the terms of reference of the privacy committee are closely modelled on the recommendations put forward in a report on the law of privacy written by Professor W.L. Morison, which was tabled in the New South Wales parliament in April 1973[170]. The Morison Report canvassed existing legal protections of privacy interests and made an appraisal of their applicability to a number of areas of activity in which invasions of personal privacy might occur. It was Morison's conclusion that because of existing and foreseeable threats to the privacy of the individual, some legislative initiative should be taken. However, in view of the "lack of development of privacy policies at the present time" and the extent to which these matters are affected by rapid social and technological change, it was recommended that, rather than create a general legal right to privacy, it would be desirable to establish a body which would attempt to mediate disputes and gather information with a view to recommending such specific legislative initiatives as might appear necessary. The Privacy Committee itself outlined the rationale for this approach to privacy protection problems in the following terms:

A general privacy law could cause uncertainty until a large body of supplementary case law develops. As a result it could be a law offering spasmodic and uneven protection. Other problems are that the social contexts of many privacy problems are little understood, the proper values of privacy are open to debate, and the field of privacy is subject to rapid social and technological change. The majority of

privacy issues can be resolved by the Committee without recourse to legal proceedings[171].

The composition of the committee is prescribed by statute, and it is composed of twelve to fifteen members, of whom one must be the Ombudsman. Of the remaining members, two are appointed by the Governor from elected members of the legislature, with one nominated by the leader of the Opposition and one by the responsible minister; two are members of the public service, two are university faculty members, and the others are persons nominated by the minister who have "special knowledge of or interest in matters affecting the privacy of persons"[172]. The committee has the power to delegate its statutory powers to subcommittees (in fact, most of the committee's statutory functions are performed at the subcommittee level). To date, the bulk of the committee's energies have been absorbed in its complaints investigation and research functions.

The committee is vested with powers similar to those of a royal commission; it may require the production of documents and the appearance of witnesses[173]. It is our understanding that, as a general rule, the power to conduct investigations is infrequently, if ever, used by the committee. The committee prefers to seek voluntary cooperation both in its investigations and in its attempts to find solutions to specific complaints.

The range of privacy protection problems examined by the committee is very broad. Since its establishment, it has considered, among other subjects, privacy protection problems arising in the course of credit reporting, law enforcement, the delivery of health care services, employer-employee relations, the activities of the press, and radio and television, the use of rights of entry, unsolicited mail and telephone calls, the use of surveillance devices and the operation of personal data banks by both private and public institutions[174]. The committee has published an illuminating and thoughtful series of more than fifty research papers, case studies, briefs, and suggested codes of practice. During the period between its establishment in 1975 and June 1978, the committee actively investigated almost 900 complaints. In only two cases were the committee's recommendations rejected.

The Privacy Committee appears to have enjoyed considerable success in achieving complaint resolution and the voluntary adoption of codes of behaviour. The committee's work thus represents an interesting experiment in the use of mediation and self-regulation as techniques for addressing privacy protection problems. Indeed, the committee has advocated the view that self-regulation undertaken in a cooperative spirit is generally a more desirable approach to the privacy issue than the adoption of

legislative schemes[175]. Although the committee has not precluded itself from recommending legislation in the future, it has not yet recommended the adoption of legislated privacy protection schemes with respect to either private or public institutions, nor has it recommended the enactment of a law establishing a general right of privacy.

Of particular interest in the present context is the approach taken by the committee to the problems of informational privacy arising in the context of personal record keeping by public and private institutions. Consistent with its approach to other areas of privacy protection problems, the committee studied a number of specific record-keeping practices and published guidelines for the operation of personal data systems[176], which it recommended for adoption by all private and public institutions operating personal data systems. These guidelines were summarized in the following terms:

The Seven Basic Principles

These are intended to guide organizations in achieving their legitimate aims without undue intrusion into people's lives. In different situations different methods of implementation of these guidelines will be appropriate.

A. The Justification for the System

1. Social Acceptability of the System's Purpose and Uses

A personal data system should exist only if it has a general purpose and specific uses which are socially acceptable.

2. Relevance and Social Acceptability of Data for Specific Decisions

Personal data should only be used when it is relevant to the particular decision being made, and its use for this decision is socially acceptable.

B. The Operation of the System

3. Data Collection

The minimum necessary data should be collected, using fair collection methods, and from appropriate sources.

4. Data Integrity, Security and Retention

Standards should be established and maintained regarding data integrity, data security and the period for which identified personal data is retained.

5. Data Access

Personal data should only be accessed consistently with the systems' socially acceptable uses, and for additional uses by consent or by law.

C. Mechanisms of Public Access

6. Public Access

The interested public should be able to know of the existence, purpose, uses and methods of operation of personal data systems; to object to any feature of a system; and where appropriate to have change enforced.

7. Subject Access

Every person should be able to know of the existence and of the content of data which relates to himself; to complain about any feature of that data or its use; and where appropriate to have change enforced[177].

A more detailed statement of these seven principles is then set forward by the committee in terms which would be very familiar to readers of the North American and European data protection literature and legislation. With respect to the collection of data, the committee recommends that the minimum data necessary to achieve the purpose is all that should be collected, and that it should be collected, where possible, from the data subject himself. In the course of the process of collection, the data subject should be made aware of the purpose and uses for which the data is collected, and should be advised of the consequences of failure to supply the information and of how he might direct an inquiry or complaint if he is dissatisfied with the collection activity. The committee has apparently enjoyed some considerable success in persuading both the government bodies and private sector institutions to adopt data protection practices in accordance with the guidelines.

CHAPTER 29 NOTES

- 1 The Swedish Data Bank Statute, 1973, c. 289, s. 2.
References in this chapter to this statute are to the English translations in Charles K. Wilk, ed., Selected Foreign National Data Protection Laws and Bills (Washington: USGPO, U.S. Department of Commerce, Office of Telecommunications, 1978), cited hereafter as Wilk, and in P.G. Vinge, Swedish Data Act (Stockholm: Federation of Swedish Industries, 1973). For a discussion of the Data Inspection Board's activities, with particular reference to statistical data, see D.H. Flaherty, Privacy and Government Data Banks (London: Mansell, 1979), Chapter 7.
- 2 Ibid., s. 3.
- 3 Ibid., Regulation of May 11, 1973, s. 2(4).
- 4 The Swedish Data Bank Statute defines the registrar-accountable as "anyone on whose behalf the register is maintained, provided that he also has control over the register." The registrar-accountable may be either a natural person or an organization. The duties of the registrar-accountable are set out in ss. 8-14 of the act.
- 5 Data Bank Statute, ss. 5 and 6.
- 6 Ibid., ss. 8-14.
- 7 Ibid., ss. 3, 5, 6.
- 8 Ibid., s. 25.
- 9 Ibid., s. 4.
- 10 Ibid., Regulation of May 11, 1973, s. 2(10).
- 11 Ibid., s. 22.
- 12 Ibid., s. 23.
- 13 Ibid., s. 24.
- 14 Ibid., s. 20.
- 15 Ibid., s. 21.
- 16 Sweden, Committee for Data Legislation (DALK), Personregister-Datorer Integritet (Stockholm: DALK, 1978).

- 17 See generally, F.W. Hondius, Emerging Data Protection in Europe (New York: American Elsevier Publishing Company Inc., 1975), Chapter 3; Report of the Committee on Data Protection (1978; Cmnd. 7341) 31-35, cited hereafter as Lindop Report.
- 18 Report of the Committee on Privacy (1972; Cmnd. 5012), cited hereafter as Younger Report.
- 19 Act Relating to Personal Data Registers, 1978, s. 9.
- 20 Ibid., s. 1.
- 21 Ibid., ss. 2, 3, 4, 5, and 9.
- 22 Ibid., ss. 13-35.
- 23 Ibid., s. 41.
- 24 Private Registers Act, 1978, No. 293, s. 3(3).
- 25 Law No. 78-17 of January 6, 1978, Concerning Data Processing, Files and Liberties, translated in Wilk, 48.
- 26 Ibid., art. 15.
- 27 Ibid., art. 16.
- 28 Ibid., art. 22.
- 29 Ibid., art. 8.
- 30 German Federal Republic, Law for the Protection of Personal Data Against Misuse in Data Processing (Federal Data Protection Law), 1977, translated in Wilk, 10.
- 31 Ibid., s. 3.
- 32 Ibid., ss. 2(2)(1) and 2(3)(3).
- 33 Ibid., ss. 7(1), 22, and 31.
- 34 Ibid., s. 7(2). The act applies to certain organizations in the absence of similar laws passed by the "Länder" (provinces): "Insofar as data protection is not governed by Land law, the provisions of this chapter...shall apply to (1) authorities and other public agencies of the Länder, municipalities and their associations, and other legal entities of public law under the supervision of the Land, and to associations if these implement federal law;

(2) authorities and other public agencies of the Länder insofar as they function as organs of the administration of justice."

35 Ibid., s. 12(1).

36 Ibid., s. 12(2)1.

37 Ibid., s. 34.

38 Ibid., ss. 13, 26, 34.

39 Younger Report, para. 621, 622. The committee also recommended that the law on breach of confidence actions be clarified and a statutory cause of action be created as a remedy for invasion of privacy.

40 Computers and Privacy (1975; Cmnd. 6353).

41 Report of the Committee on Data Protection (1978; Cmnd. 7341).

42 At the time of its report, the committee foresaw a need for thirty-seven separate data classes and fifty different codes of practice: Lindop Report, 164.

43 Ibid., 201.

44 Ibid., 202-203.

45 Ibid., 191.

46 Ibid., 175.

47 Ibid., 178.

48 Ibid., 277.

49 Ibid., 201.

50 Ibid., 226. At the time of its report, the committee noted that very little sensitive social work information was in fact stored by computer but stated that the situation would likely change in the near future.

51 Ibid., 229.

52 Ibid., 232.

- 53 Ibid., 225.
- 54 Ibid., 220-21.
- 55 Ibid., 221-23.
- 56 Ibid., 188. In practice, this appointment would be made on the advice of the Prime Minister.
- 57 Ibid., 197.
- 58 Ibid., 193. The committee recommended that the legislation allow for an appeal to the courts on a question of law from a decision of the DPA.
- 59 Privacy Act, 1974, 5 U.S.C., s. 552a, passed as part of Pub. L. No. 93-579.
- 60 Records, Computers and the Rights of Citizens (Massachusetts Institute of Technology, 1973), cited hereafter as HEW Report. See generally, Senate Committee on Government Operations and the House Committee on Government Operations, Joint Committee "Legislative History of the Privacy Act of 1974, s. 418 (Public Law 93-579)", Source Book on Privacy, September 1976.
- 61 Privacy Act, 1974, Pub. L. No. 93-579, s. 2(b).
- 62 Ibid., s. 3(g).
- 63 The PPSC was established pursuant to section 5 of the Privacy Act.
- 64 Personal Privacy in an Information Society (Washington: USGPO, 1977), cited hereafter as PPSC Report.
- 65 PPSC Report, Appendix 4, The Privacy Act of 1974: An Assessment (Washington, D.C.: USGPO, 1977) 76, cited hereafter as App. 4.
- 66 5 U.S.C. s. 552a(e)(4).
- 67 Ibid., s. (e)(3).
- 68 PPSC Report, App. 4, 8.
- 69 Ibid., 82.
- 70 Ibid., 28-29, 88-89.

71 5 U.S.C. s. 552a(d)(1).

72 Ibid., s. (a)(4).

73 Ibid., s. (a)(5).

74 PPSC Report, App. 4, 5.

75 Ibid., 6.

76 The following definition of the term "accessible record" was suggested:

(6) the term "accessible record" means an individually identifiable record, except a research or statistical record, which is

(a) systematically filed, stored, or otherwise maintained according to some established retrieval scheme or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the record, or any portion thereof, on the basis of the identity of, or so as to identify, an individual, or

(b) otherwise readily accessible because:

(i) the agency is able to access the record without an unreasonable expenditure of time, money, effort, or other resources, or

(ii) the individual to whom the record pertains is able to provide sufficiently specific locating information so as to render the record accessible by the agency without an unreasonable expenditure of time, money, effort or other resources.

77 See PPSC Report, App. 4, 9. The total number of systems exempted in this fashion would be less than this, however, since exemptions may have been claimed for the same system under several different exempting provisions.

78 PPSC Report, App. 4, 37-38.

79 5 U.S.C., s. 552(d)(2),(3).

80 Ibid., (d)(2).

81 Ibid., (d)(3).

82 Ibid., (d)(4).

83 PPSC Report, App. 4, 127-28.

84 5 U.S.C. s. 552a(e)(7).

85 Ibid., s. 7.

86 Ibid., s. (e)(1).

87 Ibid., s. (e)(2).

88 Ibid., s. (e)(3).

89 PPSC Report, App. 4, 88-90.

90 5 U.S.C. s. 552a(b)(1).

91 See PPSC Report, App. 4, 90-91.

92 5 U.S.C. s. 552a(b)(3)(a)(7).

93 Ibid., (b).

94 PPSC Report, App. 4, 91-95.

95 PPSC Report, 33-37; App. 4, 95.

96 5 U.S.C. 552a(e)(5).

97 Ibid., s. (e)(10).

98 PPSC Report, App. 4, 98-99.

99 Ibid., 97.

100 5 U.S.C. s. 552a(c).

101 Ibid., s. (c)(1).

102 Ibid., s. (c)(2).

103 Ibid., s. (c)(3).

104 Ibid., s. (c)(4).

105 PPSC Report, App. 4, 103, 122-23.

- 106 5 U.S.C. s. 552a(g).
- 107 PPSC Report, App. 4, 103-106.
- 108 Ibid., 97.
- 109 5 U.S.C. s. 552a(i)(1).
- 110 Ibid., s. (i)(2).
- 111 Ibid., s. (i)(3).
- 112 PPSC Report, App. 4, 97.
- 113 Ibid., App. 4, 39-41, and see Kentucky Legislative Research Commission, Research Report No. 145, Personal Information and Privacy (Frankfort, Ky.: 1977) 19-27 for a discussion of the cost implications of privacy protection schemes.
- 114 See Robert E. Smith, Compilation of State and Federal Privacy Laws, 1978-79 (Washington: Privacy Journal, 1978) and Privacy Protection Study Commission, Privacy in the States, Appendix 1 (Washington: USGPO, 1977).
- 115 Arkansas, Information Practices Act, Ark. Stat. Ann., s. 16-804; California, Information Practices Act of 1977, Cal. Civil Code, see s. 1798; Connecticut, Personal Data Act, Conn. Gen. Stat. Ann., s. 4-190; Indiana, Fair Information Practices Act, I.C. 4-1-6-1; Massachusetts, Fair Information Practices Act, Mass. Gen. Laws, Ann. ch. 66A, as amended; Minnesota, Data Security and Privacy Act, Minn. Stat. Ann., s. 15.162; Ohio, Personal Information Control Act, Ohio Rev. Code, s. 1347.01; Utah, Information Practices Act, Utah Code Ann., s. 63-50-1; Virginia, Privacy Protection Act, Va. Code, s. 2 1-377.
- 116 Information Practices Act, s. 16-702(e).
- 117 Personal Data Act, s. 1(i).
- 118 Privacy Protection Act, s. 2.1-379(2).
- 119 Information Practices Act, s. 1798.40.
- 120 Ibid., s. 1798.3(a).
- 121 Ibid., s. 1798.24(g).
- 122 Public Records Act, Cal. Civil Code, s. 6254(c).

- 123 Information Practices Act, s. 1798.7.
- 124 Ibid., s. 1798.9.
- 125 Ibid., s. 1798.5.
- 126 Ibid., s. 1798.6(a).
- 127 Ibid., s. 1798.8.
- 128 Ibid., s. 1798.6(b).
- 129 Ibid., s. 1798.47.
- 130 Data Security and Privacy Act, s. 15.1671.
- 131 Ibid., s. 15.169, sub. 1.
- 132 Ibid., sub. 3(1).
- 133 Ibid., sub. 3(3).
- 134 S.C. 1976-77, c. 33. Other parts of the act deal with prohibited grounds of discrimination and are of no relevance to privacy protection concerns.
- 135 Schedule 1 to the act contains a list of the government departments and institutions to which the act applies.
- 136 S. 51. The index is to be published "on a periodic basis not less frequently than once each year...."
- 137 Ibid., s. 52(1).
- 138 Ibid., s. 52(2).
- 139 Ibid., s. 58(1).
- 140 Ibid., s. 56.
- 141 See Treasury Board of Canada, Administrative Policy Manual, c. 410, 415, 420 and 425, all dated December, 1978, hereafter cited as Administrative Policy Manual.
- 142 Canadian Human Rights Act, s. 56(3).
- 143 Protection of Personal Information Regulations, SOR/79-145, February 10, 1978, ss. 26-29.

- 144 Administrative Policy Manual, c. 410, 5.
- 145 Ibid., 6.
- 146 Ibid., 7.
- 147 Ibid., 9.
- 148 Ibid., 8.
- 149 Ibid., 7.
- 150 Ibid., 11.
- 151 Administrative Policy Manual, c. 420, directive 4.1.
- 152 Canadian Human Rights Act, s. 51. The index for 1979 lists 1,500 federal information banks of which 24 have been exempted from subject access.
- 153 Ibid., s. 53. Data banks exempt under s. 53 can only contain records which would themselves be exempt under the section: Administrative Policy Manual, c. 420, directive 5.1.1.
- 154 Canadian Human Rights Act, s. 54. Before claiming an exemption under this section, government institutions must consult with the privacy coordinators of the appropriate government department, or, in the case of an exemption for national security, with the Solicitor General and the President of the Treasury Board: Administrative Policy Manual c. 420, directive 6.1.1.
- 155 Canadian Human Rights Act, s. 55. Officials of the Treasury Board are to be consulted if a government institution is contemplating using this exemption: Administrative Policy Manual, c. 420, directive 5.2.
- 156 Canadian Human Rights Act, s. 49.
- 157 Administrative Policy Manual, c. 415, s. 3.2.
- 158 Ibid., s. 4.
- 159 Canadian Human Rights Act, s. 57.
- 160 Ibid., s. 58.
- 161 Ibid., s. 59.

162 Ibid., s. 60.

163 In Ontario The Consumer Reporting Act, 1973, S.O. 1973, c. 97, and s. 231 of The Education Act, S.O. 1974, c. 109, are similar in approach to the federal legislation. These statutes will be discussed in Chapter 30.

164 Manitoba, The Privacy Act, S.M. 1970, c. 74; Saskatchewan, The Privacy Act, S.S. 1974, c. 80; British Columbia, The Privacy Act, S.B.C. 1968, c. 39.

165 S.B.C. 1968, c. 39, s. 2(2).

166 S.M. 1970, c. 74, s. 3(d); S.S. 1974, c. 80, s. 3(d).

167 There appears to be only one reported case involving these statutes. In Davis v. McArthur (1971) 17 D.L.R. (3d) 760, the plaintiff was awarded damages at trial for an invasion of his privacy by a private investigator who had attached an electronic listening device to his car. However, the British Columbia Court of Appeal reversed the decision, holding that this kind of surveillance was not unreasonable in divorce proceedings.

168 New South Wales, Privacy Committee Act, 1975, no. 37.

169 The Privacy Committee Act, s. 15, sets out the committee's powers in the following terms:

(1) Subject to this Act, the Committee --

(a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons;

(b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;

(c) may make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;

- (d) may receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;
- (e) may, in relation to any matter relating to the privacy of persons generally, disseminate information and undertake educational work;
- (f) may, in relation to any matter relating to the privacy of persons generally, make public statements; and
- (g) may, for the purposes of this Act, conduct such inquiries and make such investigations as it thinks fit.

170 W.L. Morison, Report on the Law of Privacy (Parliament of New South Wales, Australia, 1973).

171 Introducing the Privacy Committee (Sydney: Privacy Committee, 1978) 1.

172 Privacy Committee Act, s. 5.

173 Ibid., s. 16.

174 For a useful summary of the committee's work from 1975-78, see New South Wales, Privacy Committee Report 1975-78 (Sydney: 1979).

175 Ibid., 4.

176 New South Wales, Guidelines for the Operation of Personal Data Systems: Exposure Draft (Sydney: Privacy Committee, 1977).

177 Ibid., 2.



CHAPTER 30

The Legal Framework of Privacy Protection in Ontario

A. INTRODUCTION

In this chapter we examine the common-law principles and statutory provisions in Ontario that relate to personal privacy. The examination focuses on the degree of privacy protection offered by the existing law, particularly with respect to the kinds of information-handling practices outlined in Chapter 27. Certain provisions of The Consumer Reporting Act, The Education Act, and The Ontario Human Rights Code that seek to control the collection and use of personal information are also described.

B. THE COMMON LAW

Many Ontario statutes require individuals to provide information about themselves to the government in order to qualify for certain benefits or to comply with government regulatory programs. Yet Ontario has no general legislation designed to protect individual privacy or to control the use of this kind of information.

Unlike the United States, where invasion of privacy is a wrong for which the courts will give relief, in Canada the common law does not yet appear to explicitly recognize a right to privacy[1]. Therefore, there are no common-law privacy principles which can be applied to regulate the kind of information which governments (or private institutions) can collect about individuals, nor the use to which that information may be put.

The common law of torts indirectly offers limited protection to some aspects of individual privacy[2]. The old actions for trespass and nuisance may give remedies against certain methods of information collection, and the actions for libel and slander, injurious falsehood, breach of contract, breach of confidence and the willful doing of an act calculated to cause harm protect, to some extent, against the harmful use of personal information. However, these actions protect privacy only incidentally to the protection of some other more traditional interest, such as the right to undisturbed use of one's property.

The difficulties of applying these torts to the problem of regulating the collection and dissemination of personal

information by government agencies are substantial. Indeed, they must be considered only marginally relevant for this purpose. The action for trespass, for example, provides a remedy for unauthorized physical intrusion onto land. Unreasonable interference with an occupier's use and enjoyment of property will give rise to an action in nuisance. Many Ontario statutes expressly empower government inspectors to enter business premises and to seize records and documents as part of their regulatory powers[3]. Similarly, police officers have special authority to enter both business premises and private dwellings under the provincial Summary Convictions Act[4] and the federal Criminal Code[5]. These tort actions would only be available where law enforcement officials exceed their statutory powers of search and seizure. The provincial Telephone Act[6] and the federal Protection of Privacy Act[7] and Post Office Act[8] provide criminal penalties for unlawful interception of private communications, although, again, law enforcement authorities have special privileges. As a general rule, however, since evidence obtained illegally is not inadmissible in criminal proceedings under Canadian law on that ground alone, the deterrent effect of these statutory provisions is open to question.

However, most of the personal information in government records is supplied voluntarily by the record subjects themselves, and not as a result of intrusive government investigations. What protection does the common law offer to control the use or disclosure of this kind of information?

The common-law actions for libel, slander, injurious falsehood and passing off are designed to provide compensation in cases where untrue statements are publicly made and have the effect of damaging a person's business interests and reputation in the community. There are two main problems with these actions in the context of protecting informational privacy. First, if the statements are true, the actions fail; thus they are of no use in protecting against public disclosure of true personal information. Second, even if they are false, the plaintiff must show that the false statements have caused him monetary loss: injured feelings or "outraged dignity" alone are not harms for which the law will usually give redress.

The tort of willfully doing an act calculated to cause harm, first outlined in Wilkinson v. Downton[9], might be the basis for an action against a government official who publicly released private information about an individual, if the disclosure could be shown to have been intended to cause severe distress and did in fact do so.

If an express or implied term of a contract promising confidentiality is breached, the courts will give relief as they would for breach of any contractual term. However, it is difficult to classify most situations in which individuals supply information to government as giving rise to a contractual relationship, so that this cause of action would rarely be available to compensate for a breach of individual privacy by government officials.

An action for breach of confidence has been described by some commentators as offering the most effective protection for privacy available at common law[10]. It makes actionable the unauthorized disclosure or use of information which has been given in confidence. Although the modern development of this tort has occurred mainly in the context of commercial trade secrets, it has been said that:

"...the jurisdiction [to restrain publication of confidential information] is based not so much on property or contract, but rather on the duty to be of good faith"[11].

The action is not dependent on the existence of a contract and conceivably could be used against government officials who use or disclose personal information in bad faith or without consent, although there are as yet no reported cases where this has occurred. If the government could show that the breach of confidentiality was justified in the public interest, the action would fail[12].

In summary, then, Anglo-Canadian common law has not yet evolved to the point where it explicitly recognizes a right to privacy. The various tort actions described above may offer some protection to individual privacy in certain circumstances -- but only incidentally to protecting some other legally-recognized interest. The U.S. courts, by adapting common-law principles, have developed the tort of invasion of privacy as a distinct head of liability. Canadian courts have not yet followed this doctrine, although there are hints in some recent cases that the U.S. lead may eventually be followed here[13]. In the meantime, however, several Canadian provinces have established statutory causes of action for invasion of privacy (see Chapter 29 of this report).

It should be said, however, that even a fully developed tort action for invasion of privacy would not give adequate protection against some record-keeping practices. First, tort actions only provide compensation after the harm has been done. Although a sufficiently large damage award might deter government officials from repeating certain specific conduct, individual tort actions would be an expensive and time-consuming method of regulating

information practices. Second, for many people the cost of litigation makes it an impractical remedy for invasion of privacy. Third, since court proceedings are necessarily a matter of public record, taking legal action simply exacerbates the wrong for which relief is sought -- the public disclosure of confidential information. Finally, with specific reference to government record keeping, the legal and practical difficulties which confront a litigant who wishes to bring a suit against the Crown further reduce the attractiveness of this avenue of relief[14]. For these reasons, common-law tort actions are not likely to provide an effective means of regulating government record-keeping practices.

C. STATUTORY SECRECY PROVISIONS

The extensive use of secrecy provisions in Ontario statutes has been outlined in Volume 2, Chapter 7[15]. Many of these provisions, which require civil servants to maintain secrecy about all matters that come to their knowledge in the course of their duties, seem to be intended to protect the privacy of those who supply information, either voluntarily or under statutory compulsion, to the government. The adoption of these provisions has, however, developed in an ad hoc way rather than as part of an overall scheme to protect individual privacy. Thus, the same kinds of information are given inconsistent protection in different contexts. Licensing statutes and taxing statutes, for example, usually contain strict secrecy provisions, presumably to protect the confidentiality of financial information supplied by the private sector. The Health Insurance Act[16], The Cancer Act[17], and The Workmen's Compensation Act[18] all contain provisions to preserve the confidentiality of medical records. The Family Benefits Act[19], on the other hand, under which a great deal of both medical and financial information about individuals is collected by government, contains no secrecy provisions. The handling of this kind of information is left to the discretion of those government officials who possess it.

Some statutory secrecy provisions apply only to information collected by government inspectors in the exercise of their statutory powers of investigation[20]; others make no distinction between kinds of information -- they simply declare "all matters" to be secret[21].

The privacy of individuals is protected, of course, by the practice of various government departments and agencies of refraining from disclosure of personal information, a practice supported by the oaths of secrecy to which public servants are required by statute to subscribe. Secrecy oaths must be sworn by

government employees, either under The Public Service Act or under the particular statute they administer. Although there is no penal sanction provided for breach of secrecy oaths, they no doubt do encourage an atmosphere of secrecy which provides some protection for individual privacy.

The provisions in many statutes which render government officials non-compellable or incompetent witnesses in court proceedings other than those brought under the particular statute, serve to restrict access by litigants to private or confidential information in government records.

Statutes governing the procedures of boards and tribunals holding adjudicatory hearings generally grant discretion to hold hearings in camera in order to protect the confidentiality of intimate personal or financial matters[22]. Section 9 of The Statutory Powers Procedure Act, for example, allows government boards to sit in camera where they determine that the need to protect an individual's privacy outweighs the public interest in open hearings. The Criminal Injuries Compensation Board has discretion to sit in camera where the applicant for compensation is the victim of a sexual assault or where a public hearing might prejudice a party's right to a fair trial. On the other hand, the Social Assistance Review Board, which hears appeals from the decisions of the Directors of Provincial Benefits and Vocational Rehabilitation, has no discretion in this matter: by law, all its hearings must be held in camera. In this case, the legislature has decided that the interest in protecting the privacy of individuals who appear before the board always outweighs the public interest in open hearings.

In summary, then, a variety of statutory secrecy provisions do provide a measure of protection for individual privacy by restricting or prohibiting the disclosure of information to the public. Nevertheless, taken as a whole these provisions do not constitute a coherent privacy protection scheme: to discover the kind of protection afforded to particular information about individuals it is necessary to examine the specific statute under which the information is collected.

D. THE CONSUMER REPORTING ACT AND THE EDUCATION ACT

Two statutory schemes which do address informational privacy concerns have been enacted in Ontario. The Consumer Reporting Act[23] and The Education Act[24] illustrate the use of legislation in Ontario to regulate the use and transfer of information about individuals. By placing limits on the dissemination of personal information and by giving record subjects the right to

examine and correct file information, these statutes provide a measure of protection for personal privacy in two contexts: consumer credit reports and student records.

THE CONSUMER REPORTING ACT

The Consumer Reporting Act of 1973 was the culmination of a series of legislative attempts (begun in 1971) to regulate the activities of private sector agencies which supply information about individuals at the request of third parties[25].

Although the tremendous expansion of consumer credit in the 1960s increased credit grantors' use of these agencies, they are not the exclusive users of reports containing personal information. Investigative reports are also used by employers, insurers, and landlords, among others. News stories and academic studies reporting the misuse of personal information led to an increased public awareness of the potential for invasion of privacy, a potential which was further compounded by rapid computerization of industry record holdings[26].

In summary, the act requires all private sector agencies engaged in collecting and supplying information about "consumers" [27] to register with the government; it imposes some restrictions on the kinds of information which can be recorded and to whom the information can be supplied; it imposes an obligation on some users of information to notify the consumer that he is being investigated; and it gives the consumer the right to examine and correct information in an agency's records.

Registration

The act requires that all private sector agencies which investigate and report on consumers to third parties register with the Registrar of Consumer Reporting Agencies in the Ministry of Consumer and Commercial Relations[28]. They are therefore subject to the supervision of the registrar who has the power to refuse or to revoke a licence on the grounds of an agency's financial instability or illegal or unethical practices[29].

Collection and Dissemination of Information

Agencies are subject to certain restrictions on the kinds of information that can be reported about consumers[30]. The reporting of a consumer's race, creed, colour, sex, ancestry, ethnic origin or political affiliation is prohibited[31]. Criminal

charges that have been dismissed, set aside or withdrawn cannot be reported[32]. Records of debts that are no longer outstanding or are statute-barred must be deleted[33]. Uncorroborated information that reflects "unfavourably" on a consumer's character, reputation, health, physical or personal characteristics, or mode of living may, however, be reported as long as the agency makes "reasonable efforts" to corroborate it and the absence of corroboration is noted in the report[34]. The widespread criticism about the use of hearsay evidence in investigative reports apparently had little impact on this aspect of the legislation[35].

Agency dissemination of information about consumers is restricted to those who have a "direct business need" for it[36]. This includes credit grantors, employers, landlords, insurers and anyone who "intends to use the information to determine the consumer's eligibility for any matter under a statute or regulation"[37]. An exception to the general rule of "direct business need" is made for police and government authorities: agencies have discretion to disclose to them the names, addresses and places of employment of consumers[38]. Access to information beyond this kind of identifying material is presumably available only to police and governments by court order.

A further restriction on disclosure appears in section 10(5), which prohibits credit grantors from passing on unfavourable information about a customer's character, reputation, health, physical or personal characteristics or mode of living to other credit grantors or consumer reporting agencies unless the consumer consents or unless he is informed at the time of the application for credit that this will be done. Refusing to agree to these terms may result in the denial of credit. If the credit market is tight, or if this practice is universal in the industry, the consumer will have little control over the dissemination of this kind of information. Therefore, the right to examine and make corrections to agencies' records assumes even greater importance.

Obligations on Users of Reports to Give Notice to Consumers

The act imposes certain obligations on users of agencies' reports to give the consumer notice that an investigation has been or will be conducted. Credit grantors who are using or who intend to use a report containing "credit information" are obliged to so notify the applicant for credit at the time the application is made[39]. They need not disclose the name of the agency to be used unless the applicant requests this information. Any other users of credit information need only inform the consumer of the fact that he is being or has been investigated, and the name of

the agency, if he asks[40]. However, no one is permitted to request or make use of any agency report containing "personal information" unless the consumer is given advance notice of the fact that this will be done[41]. Again, the name of the agency need only be disclosed if the consumer asks for it. These notice provisions, however, do not apply to any user of information who intends to seek any information from sources other than consumer reporting agencies. Apparently, many credit grantors as well as landlords, employers, and insurers do not use reporting agencies but conduct their own investigations[42]. In these cases, the consumer need not be informed of the fact that an investigation has been carried out unless a decision adverse to the consumer is made on the basis of the information thus obtained[43]. In that case, the user must so inform the consumer. In addition, the user must notify the consumer of his right to be informed of the nature and source of the information. Similarly, if damaging information is obtained from a consumer reporting agency, the consumer must be informed of that fact and of his right to be told the name of the agency.

Access Rights to Agency Records

The obligations on agencies to disclose information to consumers are fairly extensive, for those who take advantage of their rights[44]. Upon presenting proper identification, a consumer, alone or accompanied by a person of his choosing, is entitled to be informed of the nature and substance of all information in his file, or the sources of credit information (sources of "personal information" remain confidential), and of the names of those to whom the agency has supplied information about him. He is entitled to make abstracts of this information and to receive copies of all reports which have been sent out about him, including those purporting to describe his character, reputation, mode of living and so on. An exception is made for medical reports, which the agency has obtained from his own doctor with his consent, if the doctor states in writing that the report should be withheld "in [the consumer's] own best interest"[45].

In addition, the agency must provide trained personnel to assist the consumer in understanding the material. Furthermore, it must advise him of his rights with respect to seeking correction or deletion of material in the file. If the consumer and the agency cannot agree on corrections, the consumer may appeal to the registrar to resolve the dispute[46]. A second appeal is available for either the consumer or the agency to the Commercial Registration Appeal Tribunal (CRAT), at which point a hearing will be held. The tribunal has power to order the agency to disclose the sources of its "personal information" about the

consumer[47]. Where corrections are ordered to be made either by the registrar or by CRAT or are agreed to between the consumer and the agency, the agency has a duty to notify past recipients of the incorrect reports and of the amendments which have been made[48].

THE EDUCATION ACT

Section 231 of Ontario's Education Act places restrictions on the use of information contained in school records and gives parents or pupils rights of access and correction and a measure of control over their use[49]. In the United States the unauthorized use of information contained in school records has led to several successful damage suits, and the enactment of section 231 was largely in response to concerns expressed by Ontario school boards and teaching staff about their own potential liability. The act prohibits any action against any person in respect of the content of a record[50].

Section 231 applies to the Ontario Student Record (OSR) which is maintained by principals on every elementary and secondary student in the province. The section declares the records to be "privileged for the information and use of supervisory officers and the principal and teachers of the school for the improvement of instruction of the pupil." Disclosure to outsiders without the written permission of the parent, or the pupil if he is an adult, is prohibited[51]. However, there are exceptions to this non-disclosure rule. Information which may be required by the Minister of Education or the school board may be supplied by the school, apparently without the knowledge or consent of the student or parents[52]. The contents of school records are declared to be inadmissible as evidence in legal proceedings, other than internal disciplinary proceedings brought by the principal, without the written permission of the parent or pupil[53]. The intention of the section, then, is to limit the use of school records to the purposes of the educational system itself[54].

A pupil (or his parent or guardian if he is a minor) has the right to examine his school record and to request that information which is inaccurate or is "not conducive to the improvement" of the pupil's instruction be amended or deleted[55]. If the principal refuses to comply, the matter must be referred to a supervisory officer who has the power either to order the principal to comply or to submit the dispute to an arbitrator designated by the minister. The arbitrator must then hold a hearing and his decision is final and binding on the parties[56].

E. THE ONTARIO HUMAN RIGHTS CODE

The Ontario Human Rights Code was first enacted in 1962[57]. Its purpose is to prevent discrimination against individuals or classes of individuals, particularly in housing or employment, on the basis of race, creed, colour, sex, nationality, ancestry, place of origin, age or marital status. Under the code, employers are prohibited from requiring an applicant for employment to furnish any information concerning race, creed, colour, nationality, ancestry or place of origin[58]. This provision of the code restricts the kind of personal information which can be collected by prospective employers in both the public and private sector in Ontario.

CHAPTER 30 NOTES

- 1 The American development of tort principles to recognize a right to privacy was substantially influenced by the famous article by Warren and Brandeis, "The Right to Privacy," (1890) 4 Harv. L. Rev. 193.
- 2 See T.G. Brown, Government Secrecy, Individual Privacy and the Public's Right to Know: An Overview of the Ontario Law, (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 11, 1979), hereafter cited as T.G. Brown; John G. Fleming, The Law of Torts, 4th ed. (Sydney: The Law Book Co. Ltd., 1971).
- 3 For example, The Liquor Licence Act, S.O. 1975, c. 40, ss. 21-23; The Travel Industry Act, S.O. 1974, c. 15, ss. 17-20.
- 4 R.S.O. 1970, c. 450, s. 16.
- 5 R.S.C. 1970, c. C-34, ss. 443-6.
- 6 R.S.O. 1970, c. 457.
- 7 Incorporated into the Criminal Code, R.S.C. 1970, c. C-34 as Part IV.1, ss. 178.1-178.23.
- 8 R.S.C. 1970, c. P-14, s. 58.
- 9 [1897] 2 Q.B. 57.
- 10 See Report of the Committee on Privacy, (1972; Cmnd 5012) 26.
- 11 Fraser v. Evans [1969] 1 Q.B. 349 at 361 (Lord Denning).
- 12 In Initial Services v. Putterill, [1968] 1 Q.B. 396, the public interest defence was used to justify the release of confidential information which showed that a group of firms had acted contrary to the U.K. Restrictive Trade Practices Act.
- 13 See, for example, Krouse v. Chrysler Canada Ltd. (1970) 12 D.L.R. (3d) 463, Motherwell v. Motherwell (1976) 73 D.L.R. (3d) 62, Burnett v. The Queen et al. (1978) 23 O.R. (2d) 109, discussed in T.G. Brown, 214-18.
- 14 See T.G. Brown, 199-200.
- 15 Also see, generally, T.G. Brown.

- 16 S.O. 1972, c. 91.
- 17 R.S.O. 1970, c. 55.
- 18 R.S.O. 1970, c. 505.
- 19 R.S.O. 1970, c. 157.
- 20 For example, The Petroleum Resources Act, 1971, S.O. 1971, Vol. 2, c. 94, s. 5.
- 21 For example, The Upholstered and Stuffed Articles Act, R.S.O. 1970, c. 474, s. 9a, as amended by S.O. 1971, c. 50, s. 84(5).
- 22 For a description of the practices of adjudicatory boards, see Volume 2, Chapter 8, Section C of this report, and L.M. Fox, Freedom of Information and the Administrative Process, (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 10, 1979).
- 23 S.O. 1973, c. 97, proclaimed in force on July 2, 1974.
- 24 S.O. 1974, c. 109, s. 231, which first appeared in S.O. 1972, c. 77, s. 14 as an amendment to The Schools Administration Act and was later incorporated into The Education Act.
- 25 See generally, Jacob S. Ziegel, "Canadian Consumer Reporting Legislation: Trends and Problems," (1973) 11 O.H.L.J. 503, hereafter cited as Ziegel.
- 26 Ibid., 503-504.
- 27 S. 1(a). Excluded from coverage are small businessmen and professionals.
- 28 S. 3.
- 29 S. 4.
- 30 S. 9.
- 31 S. 9(3)(1).
- 32 S. 9(3)(j).
- 33 S. 9(3)(c)-(g).
- 34 S. 9(3)(b) and s. 1(1)(j).

- 35 Ziegel, 511.
- 36 S. 8(1)(d)(vi).
- 37 S. 8(1)(d)(i)-(v).
- 38 S. 8(3).
- 39 S. 10(3). "Credit information" is chiefly factual
information such as marital status, name of spouse, number of
dependents, employment history, and state of indebtedness:
s. 1(1)(d).
- 40 S. 10(1).
- 41 S. 10(2). "Personal information" is information about a
"consumer's character, reputation, health, physical or
personal characteristics or mode of living or about any other
matter concerning the consumer": s. 1(1)(j).
- 42 Ziegel, 509, note 46.
- 43 S. 10(7).
- 44 S. 11.
- 45 S. 11(2).
- 46 S. 12.
- 47 S. 13.
- 48 S. 12(3).
- 49 For a fuller discussion of student records see M. Brown
et al., Privacy and Personal Data Protection, (Toronto:
Commission on Freedom of Information and Individual Privacy,
Research Publication 15, 1980) hereafter cited as M. Brown;
and see Chapter 27 of this report.
- 50 S. 231(8).
- 51 S. 231(2).
- 52 S. 231(7).
- 53 S. 231(2) and (13).

- 54 For a description of the effectiveness of these provisions,
see M. Brown, Part B, 14 et seq.
- 55 S. 231(3) and (4).
- 56 S. 231(5).
- 57 R.S.O. 1970, c. 318 as amended.
- 58 Ibid., s. 4(4).

CHAPTER 31

The Need for Reform

In recent history, the private lives of citizens of modern industrialized countries have come under increasingly close scrutiny by public and private institutions. As we have indicated in Chapter 25 of this report, it is our view that the growth of institutional information-gathering activities or "data surveillance" tends to pose serious risks to the preservation of personal privacy. Although it is true that some degree of encroachment on personal privacy is a price which must be paid for social and economic progress, it is also true that uncontrolled growth in institutional scrutiny of private lives would erode personal autonomy and undermine the value traditionally placed on the integrity and freedom of the individual in democratic political systems.

The informational privacy problem, like many other problems faced by developed nations, appears to result from the cumulative effect of the efforts of large institutions to respond to increasing demands for products and services. Thus, the growing use of large personal information systems and modern information technology represents, in the main, attempts to cope with the administrative burdens imposed by contemporary forms of social organization, rather than a concerted effort by the managers of personal data systems to engage in oppressive forms of social control. Nevertheless, the fact that the risks to personal privacy arise primarily by inadvertence is not a reason for ignoring the gravity of these risks or failing to respond to them by the establishment of safeguards for the public interest in the protection of personal privacy.

The essence of the informational privacy problem is the loss by individuals of control over the use and dissemination of information concerning their personal lives. The informational privacy value is depreciated when individuals are required to disclose information to another person or institution, and by a loss of control over subsequent uses made of that information. A privacy protection policy intended to preserve informational privacy would therefore attempt to restrict personal data-gathering activity to that which appears to be necessary to meet legitimate social objectives, and would attempt to maximize the control that individuals are able to exert over subsequent use and dissemination of information surrendered to institutional record keepers.

In Chapter 29, we examined the extent to which informational privacy values are dealt with in the privacy protection laws adopted in recent years by a number of North American and European jurisdictions. As our discussion indicates, these jurisdictions have adopted a variety of institutional mechanisms designed to accomplish the following objectives:

- . restraint in the collection of personal data;
- . public knowledge of the existence and nature of information systems containing personal data;
- . the securing of rights of data subjects to obtain access to and seek correction of records containing personal information;
- . the establishment of mechanisms for enabling the data subject to participate in decisions made with respect to subsequent use and dissemination of stored data;
- . the imposition of standards of data management to ensure that sensitive personal information is stored in a manner which ensures its integrity and security.

In short, these jurisdictions have established means for ensuring that "fair information practices" are observed by those institutions whose record-keeping practices have been subjected to regulation.

A major part of the study undertaken by our Commission was an examination of the personal information-handling practices of provincial governmental institutions and the laws of Ontario pertinent to the informational privacy issue. In Chapters 27, 28 and 30 of this report, our findings with respect to these matters have been set forth in detail. The substance of our conclusions is that informational privacy values are neither adequately protected by law in Ontario nor adequately implemented in administrative practices relating to the establishment and operation of personal data information systems.

Although the province of Ontario has enacted legislation implementing fair information practices in consumer credit reporting activity and in the maintenance of primary and secondary school records, the government has not enacted legislation requiring provincial governmental institutions to operate personal data systems in accord with these principles. Various statutes specifically provide for the confidentiality of a particular type of record containing personal information, but these provisions do

not appear to be influenced by a general or consistent policy relating to the protection of personal privacy.

Our examination of government record-keeping practices suggests that the informational privacy problem is similar to that found in studies of government information-handling practices undertaken in other jurisdictions. Like all modern governments, the government of Ontario is collecting increasingly large amounts of sensitive personal information concerning residents of the province. Unlike jurisdictions which have enacted data protection laws, the government of Ontario does not appear to have adopted a clear policy imposing limits on data collection activity or a systematic method of reviewing collection practices to ensure that sensitive personal data is gathered only where necessary. The Ontario government does not routinely make available information concerning its personal data banks. As we have indicated earlier, there appears to be no authoritative source of information with respect to the various kinds of data banks maintained by governmental institutions. Further, in most of the areas of governmental activity examined by our research staff, there are no policies enabling individuals to see government files containing personal information relating to themselves, or to seek correction of erroneous information. There is also an apparent absence of consistent policy with respect to the transfer and dissemination of personal information by provincial government bodies. Although there is evidence of a general reluctance to disclose personal information to outsiders, the sharing of personal data among various governmental institutions is a phenomenon noted in many of the case studies undertaken by our research staff.

Our examination of current practice also indicates that the province of Ontario, again like other large modern governments, is making increasingly extensive use of sophisticated computer technology in the design and implementation of its information systems. In Chapter 26 of this report, we briefly described the recent history of the development of computer technology and its implications for the protection of personal privacy. Although there are, of course, substantial benefits to be derived from such technology, uncontrolled growth of the use of automated personal data information systems does create a number of identifiable privacy risks. Many of the virtues of such systems, such as their enormous capacity to store and disseminate data, must be viewed as something of a mixed blessing from a privacy protection perspective. Moreover, reasonable projections of predicted growth in the technological capacity of computerized information systems threatens to remove, in the near future, many of the cost disincentives which now act as a restraint on the growth of government personal data systems. The problem of ensuring adequate security in automated data systems has been the subject of much recent

publicity. As we have indicated, however, the use of computerized information systems also affords some opportunity for the adoption of security devices which may be more effective than those feasible for manual information systems.

Apart from these concerns, it is of interest to note that the increased capacity for storage and retrievability offered by computerized information systems changes, in an important way, the character of records previously considered to be in the public domain. For example, the criminal records of individuals who have been prosecuted for offences have always been contained, in a sense, in the public records of the court system. It would be impractical, however, for members of the public to attempt to learn of the past wrongdoing of neighbours, colleagues or friends through such an enormous mass of public records. The computerization of criminal record information, however, drastically alters the accessibility of this information. If access to the system were granted to the public, the protections to individual privacy inherent in the burdensome nature of the task of uncovering a criminal record would be eliminated. Similarly, conversion to a computerized system has altered the character of public property security registers relating to the indebtedness of individuals who have purchased goods on credit. Before computerization, it would have been virtually impossible, in a large urban centre, for a curious neighbour to determine the level of one's outstanding secured debt. This is no longer the case. In short, the automation of records previously considered part of the public domain may require reconsideration of the kinds of information which should remain publicly available in this new and readily accessible form.

Although it is our view that the informational privacy problem manifest in the record-keeping practices of provincial government institutions is a serious one, we do not wish to exaggerate the scale of the problem or the gravity of the immediate risks to fundamental democratic values. A review of the case studies undertaken by our research staff will indicate that government data surveillance practices in Ontario do not to any meaningful degree approximate the nightmarish vision of a "surveillance society" portrayed by George Orwell in his famous book, 1984. Nonetheless, as technological barriers to the accomplishment of so disastrous a state of affairs are removed, we believe that it is especially important that the future growth and use of data surveillance by governmental institutions be informed by a clear perception of the risks to personal privacy, and that it be restrained and regulated by the implementation of mechanisms ensuring that fair information practices are observed by the managers of personal data systems.

As we observed in the context of our discussion of freedom of information, we believe that the substantial reform of government information practices is not a contentious matter. Virtually all of the study groups who have examined these problems in Ontario and elsewhere in the Western world have concluded that a substantial departure from traditional policies and practices is needed to meet the threat to informational privacy posed by modern personal information systems; however, there are differences of opinion as to the manner in which such change should be implemented.

Our view is that a data protection scheme along the lines developed at the federal level in Canada and the United States and in various other jurisdictions should be adopted by the government of Ontario. The essential features of such a scheme would be the following:

- the establishment of statutory duties requiring governmental institutions to abide by fair information practices;
- the establishment of a mechanism for ensuring that government data banks operate in accord with these statutory duties;
- the establishment of a satisfactory means of resolving disputes between individuals and governmental institutions relating to informational privacy questions.

In subsequent chapters of this report, we will indicate in detail the nature of the scheme we propose for enactment.

There are, however, a number of other possible methods for attempting reform of government information practices which might be considered by some observers to be satisfactory alternatives for accomplishing the same ends. It will be useful, therefore, to briefly indicate the nature of these alternatives and our reasons for favouring the adoption of a data protection law as the most desirable means of achieving effective reform.

Three alternatives are commonly discussed as possible means of implementing a privacy protection policy. First, it is sometimes suggested that the enactment of legislation recognizing the existence of a right to privacy, and stipulating that violation of that right would entitle the affected individual to seek compensation in monetary damages, would secure proper redress for privacy-invasive information-handling practices. In Chapter 30 of this report, we have explored this alternative and have put

forward our reasons for concluding that the adoption of such legislation would not constitute an adequate response to the informational privacy problems presented by government record-keeping practices. First, it is doubtful that the statutory recognition of a "right to privacy" would create a remedy for many of the privacy-invasive record-keeping practices identified in this report as matters of concern. Further, the significant cost and the uncertainty of success in bringing such claims would likely discourage aggrieved individuals from using a remedial device of this kind. In any event, the granting of some form of monetary compensation for invasions of privacy will not invariably undo the harm done by, for example, improper disclosures of sensitive personal information. Further, the adoption of a technique permitting only "after-the-fact" remedies would do little to ensure the successful implementation of privacy protection principles in the design and establishment of government personal information systems.

A second method of effecting reform which would avoid the substantial cost of litigation would be the establishment of an informal complaint handling or dispute resolution mechanism similar to the office of the Ontario Ombudsman. As we noted in Chapter 29, a device of this type has been adopted in Australia in the establishment of the New South Wales Privacy Committee. Our own view is that although the performance of functions similar to those of the New South Wales Privacy Committee would form a useful adjunct to a data protection scheme, we do not feel that it is a desirable substitute for more comprehensive regulation of government personal record-keeping practices. Although complaint resolution may effectively serve the interests of an aggrieved individual in a particular case, it is not likely to ensure the uniform adoption of fair information practices throughout the entire range of governmental information-gathering activity. It is to be noted that the New South Wales Privacy Committee was given a very broad mandate to consider privacy protection problems in a general sense. The committee is not restricted to what has been referred to in this report as the informational privacy problem, nor are they restricted to public sector privacy issues. In part, the use of this particular means for addressing privacy protection problems appears to have been the result of a concern that it would be impossible to enact a code of statutory obligations that would deal satisfactorily with the broad range of privacy protection issues arising out of modern social conditions. The mandate of the Privacy Committee is essentially to respond to complaints from members of the public and to conduct investigation and research. The threat to informational privacy values posed by government personal data systems is merely one of a number of issues on the committee's agenda. The difficulty in attempting to articulate general propositions of universal application with

respect to privacy protection questions suggests that a body with so broad a mandate would wisely be established with responsibility to engage in further research. If, however, attention is directed exclusively to the informational privacy problems inherent in government record-keeping practices, we believe that it is possible to construct a set of policies to which all governmental institutions should adhere. Accordingly, it is our view that the path of reform should lie in the direction of establishing an appropriate mechanism to ensure the implementation of such policies throughout the provincial government. We do not feel that the establishment of a body whose powers extend only to complaint resolution and research and investigation would adequately accomplish this end.

The third alternative to a statutory data protection scheme which must be considered is the possibility of achieving effective implementation of fair information practices through the adoption of administrative guidelines or similar mechanisms which would not have binding effect. Here we confront a policy choice similar to that faced in designing our proposed freedom of information scheme. Our reasons for favouring a legislated solution to the informational privacy problem are similar to those which led us to conclude that a freedom of information law would be a more satisfactory solution to the problem of securing greater openness in government information practices than would the adoption of internal administrative guidelines. First, the desirability of an administrative response to these problems rests, in part, on an assumption that flexibility in the implementation of such schemes is both necessary and desirable. As we have indicated above, however, we believe that a statement of general policy can be achieved which will satisfactorily respond to the record-keeping needs of the various institutions of the provincial government. To this extent the need for flexibility is not as great as may at first appear. Moreover, we believe the implementation mechanisms which will be further described in the course of setting forth our recommended scheme will adequately meet genuine needs for flexibility. There are, on the other hand, a number of advantages to be derived from a statutory scheme. The enactment of legislation would ensure the adoption of uniform policies and practices throughout provincial governmental institutions with respect to the specific duties imposed by statute. The creation of statutory rights would provide an effective means of redress for individuals whose privacy has been invaded by the adoption of improper information practices. The enactment of a data protection law would provide irrefutable evidence of the commitment of the government to the adoption of fair information practices in its use of data surveillance techniques. In resolving an issue which reaches so deeply into the fundamental nature of the relationship between citizens and their government, it is appropriate that the relationship between the powers of government and the rights of

individuals be precisely and clearly stated in a legislative enactment.

In the next chapter of this report, we shall describe the main features of our proposed data protection scheme.

The Proposed Legislation: A General View

Our discussion in this chapter focuses on three major aspects of the proposed scheme: first, the manner in which it is proposed to implement a statutory code of fair information practices and the objectives the code is designed to serve; second, the proposed coverage of the legislation in terms of the governmental institutions which would be brought within its scope and the kinds of information-handling activities which would be subject to regulation; third, the nature of the administrative and enforcement mechanisms necessary to implement the proposed privacy protection scheme.

A. STATUTORY IMPLEMENTATION OF FAIR INFORMATION PRACTICES

The central purpose of the proposed privacy protection scheme is to ensure that the principles of fair information practices are observed by the provincial government in its collection, storage, use and dissemination of personal information. Broadly speaking, four separate objectives are served by the scheme. The first objective is to reduce the intrusiveness of personal data collection practices; the second is to ensure fairness in decision-making with respect to individuals; the third is to permit the individual data subject to exert some control over uses made of personal data; the fourth is to ensure that reasonable expectations with respect to the confidentiality of such data will be met by the governmental institution which has collected it.

The most successful method of reducing the intrusiveness of data collection, of course, would be to reduce the extent to which data is collected in the first place. We shall make recommendations for the establishment of mechanisms to ensure that the privacy implications will be carefully weighed when decisions to gather data are initially taken. In general, however, we believe that the intrusiveness of data collection practices can be reduced by ensuring that data subjects are adequately informed of the nature of government personal data banks and, in particular, of the terms and conditions under which a given item of information will be stored and used by the institution in question. Our proposed scheme would require information of this kind to be communicated to data subjects.

The objective of securing fairness in decision making concerning individuals can be achieved by ensuring that decisions

based on personal information are made using information that is as accurate and relevant to the matter in question as is practicable. To achieve this objective, we propose that a general duty be imposed on institutions to maintain personal information in accord with standards of this kind. Further, we propose that in proper cases individual data subjects be granted the right to obtain access to records containing personal information and to seek its correction in cases where they believe it to be false. In addition, we propose that a duty be imposed on governmental institutions to correct erroneous information where it has been previously disseminated.

The third objective of permitting the individual to assert some control over the uses made of personal information concerning himself can be achieved by the imposition of controls over the use and dissemination of personal data. Although, as will be seen, there are a number of situations in which we envisage that further use or dissemination of personal data should be permitted, it is our recommendation that apart from such cases, further dissemination or use should occur only with the consent of the data subject. To some extent, then, the individual will be entitled to participate in decisions made with respect to the use of personal data.

The fourth objective of ensuring that the confidentiality of personal data is maintained by governmental institutions is achieved, in part, by the imposition of controls on dissemination and use of personal data. Apart from exceptional cases, the individual will be assured that personal information gathered for one purpose will not be used for another purpose unless the individual has consented to the subsequent use of the data. Additionally, however, we shall make recommendations with respect to the precautions to be taken to ensure the security of records containing personal information. In this way, an attempt will be made to ensure that subsequent dissemination or use of the data will not occur through an improper penetration of the information system by unauthorized individuals.

In the next chapter of this report, our specific recommendations with respect to the duties to be imposed on governmental institutions and the corresponding rights to be conferred on data subjects will be described in detail.

B. COVERAGE OF THE LEGISLATIVE SCHEME

In determining the scope of regulation in these privacy protection proposals, the kinds of institutions whose record-keeping practices will be subject to the regulation and the kinds

of record-keeping activity that will bring into operation the duties imposed by the scheme must be identified.

As with our freedom of information proposals, it is our view that the institutional coverage of the scheme should extend to those kinds of public institutions which would normally be perceived by the public to constitute a part of the institutional machinery of "government" in the broad sense. In Volume 2, Chapter 11 of this report, we indicated the difficulties involved in fashioning a satisfactory definition of governmental institutions, and we made proposals which we believe establish a satisfactory criterion for identifying those institutions. We believe that the coverage of the privacy protection scheme should be identical to that of the freedom of information law and therefore recommend that this definition be adopted for the purposes of both schemes.

As we have indicated, the informational privacy problems arising from the personal information systems of large organizations are not restricted to the record-keeping practices of governmental institutions. We believe that problems of the kind addressed in our recommendations are also to be found in the practices of non-governmental bodies. We therefore recommend that privacy protection issues relating to private sector activity be the subject of continuing study with a view to determining whether and by what means fair information practices or requirements should be extended in their application to non-governmental organizations. We shall return to this point in describing the role we envisage for the Data Protection Authority, a body whose establishment we recommend for the general purpose of supervising implementation of the privacy protection scheme.

The scope of the act's coverage with respect to the kinds of record-keeping activity that should be subject to regulation raises more subtle issues. As a preliminary point, we reiterate here that our examination of the privacy protection implications of government information practices indicates that privacy values are significantly imperilled by both manually-operated and computerized personal information systems. Accordingly, it is our view that the privacy protection scheme should apply to personal records, regardless of the method of storage. A more difficult question, however, is that of the kinds of records that should be subjected to regulation. Although it may be said in very general terms that this scheme is to apply to institutions engaged in the maintenance of records containing personal information about identifiable individuals, a more precise definition will be necessary with respect to the various duties imposed under the privacy protection scheme. For example, it is our view that each institution should be required to prepare an annual notice

containing certain information relating to personal systems or data banks. Clearly, this obligation should be imposed only with respect to collections of records containing personal information which are systematically stored and retrievable on the basis of the identity of record subjects. Personal information stored in records not maintained in such a system would not be subject to this "system notice" requirement. On the other hand, it is our recommendation that individuals be granted a more general right of access to government files containing personal information pertaining to themselves. For reasons to be explained in greater detail in the next chapter of this report, it is important that this particular right extend to all personal records which are reasonably accessible, either because they are contained in a personal data bank and can therefore be easily retrieved, or because the individual requesting the record can specifically identify the record in such a way as to enable an employee of the institution to find the record with reasonable effort. Thus, the duty imposed on governmental institutions to grant access to personal records will extend not only to records maintained in data banks but to accessible records more generally. In this respect, the subject access rights conferred under our privacy protection proposals are parallel to the general rights of access conferred under our freedom of information proposals. As we will indicate, experience in the United States in implementing the provisions of the Freedom of Information Act and the Privacy Act of 1974 indicate that a parallelism of this kind is necessary in order to effect a satisfactory integration of the two schemes.

In summary, then, although the privacy protection scheme will apply generally to records containing personal information, a number of the duties imposed by the scheme on governmental institutions will apply only to the operation of personal data systems or data banks.

C. ADMINISTRATION AND ENFORCEMENT

Two different kinds of administrative mechanisms are required for the implementation of a data protection scheme. First, some means must be established for resolving disputes between data subjects and governmental institutions maintaining personal records. For example, an individual may seek access to a record containing personal information which the government institution believes to be exempt from the general rule. The resolution of such disputes, we believe, can best be effected through the mechanisms recommended under our freedom of information proposals.

The second category of administrative tasks relates to the establishment of personal data banks in accord with the standards

for operating such systems set forth in the data protection scheme. For example, governmental institutions will be required to make appropriate arrangements for the security of data banks containing personal information. Further, a duty is to be imposed requiring that such data banks contain only such personal information as is necessary to effect the administrative purpose for which the data bank is established. Under the U.S. Privacy Act of 1974, such duties are enforceable upon judicial review and it is therefore possible that an established data bank will be found to have contravened its statutory duty and be required to revise its operations. It is our view that compliance with such duties would be more successfully and efficiently accomplished if approval of the terms and conditions under which a particular data bank is to operate could be secured at the time when the system is first established. We recommend that a Data Protection Authority charged with the responsibility of implementing this aspect of our proposals be established. The functions to be performed by the proposed Data Protection Authority and its composition are described in Chapter 34.

Subsequent chapters of the report will consider related privacy protection questions. In Chapter 35, we shall make recommendations with respect to compensation for individuals whose privacy has been invaded through breach of the obligations imposed by the scheme and the imposition of sanctions against individuals engaging in conduct which would seriously undermine the effectiveness of the proposed legislation. In Chapter 36, we return to the question of the use of standard identifiers and, in particular, the use of the Social Insurance Number by provincial governmental institutions. In Chapter 37, the question of permitting the sale of mailing lists for commercial or other purposes is considered. Chapter 38 deals with the privacy protection implications of transborder data flows, that is, the transfer of personal data beyond the boundaries of the province of Ontario.

D. RECOMMENDATIONS

In summary, then, we make the following general recommendations with respect to the enactment of a privacy protection scheme:

1. The legislation should impose duties on governmental institutions to adopt fair information practices with respect to the collection, storage, use and dissemination of personal information.
2. The privacy protection legislation should apply to the institutions of provincial government and local government bodies

in accord with the definitions of such institutions set forth in our freedom of information proposals.

3. The resolution of disputes between data subjects and governmental institutions should be effected through the same appeal mechanisms as we have recommended with respect to the freedom of information scheme; that is to say, aggrieved citizens should be entitled to seek the intervention of the Director of Fair Information Practices and to exercise rights of appeal to the Fair Information Practices Tribunal.
4. A special-purpose administrative body, the Data Protection Authority, should be established for the purposes of applying statutory standards relating to the management of personal data systems to specific data-handling processes, and of engaging in a broad research and advisory role with respect to privacy protection problems in both public and private sector record-keeping practices.

The Statutory Implementation of Fair Information Practices

INTRODUCTION

In essence, our proposals would give legislative force to the principles of fair information practices on which much of our discussion of privacy protection issues has been based. In developing these proposals, we have benefited from the experience of other jurisdictions. In particular, we have carefully examined the recent experience in Canada (under the Canadian Human Rights Act, Part IV)[1] and in the United States (under the Privacy Act of 1974)[2]. We have referred to the detailed standards developed by the Treasury Board of Cabinet; these have been developed to implement the principles of fair information practices. The U.S. experience under the Privacy Act of 1974 has been documented and examined in depth by the Privacy Protection Study Commission (PPSC). Frequent reference will be made in this chapter both to the Treasury Board guidelines[3] and to the PPSC report[4]. In addition to these sources, we have also examined, to the extent possible, the experience of other jurisdictions. In particular, we have derived much assistance from the proposals of the English Data Protection Committee[5] in fashioning a role for our proposed Data Protection Authority (DPA)[6].

As will be seen, we feel that the experimentation of other jurisdictions with the regulation of data-gathering activity by government has matured to the point where general standards of fair information practices can be articulated with some confidence. Accordingly, we believe that it is both possible and desirable to establish a detailed statutory framework for the regulation of these practices. In certain instances, it is desirable to maintain a more flexible mechanism for adjusting the general principles to specific applications. Accordingly, we shall discuss the proposed powers of the Data Protection Authority to authorize certain types of activity in accord with the general principles set forth in the statute.

In the following sections of this chapter, we set out our proposals with respect to the following matters:

- a public record of government-held personal data banks;
- controls on the collection of personal information;

- terms and conditions for the maintenance of data and the preservation of its security;
- controls on the transfer of personal data;
- subject access and correction rights;
- limitations on the uses of research and statistical data;
- the imposition of a duty to maintain a record of disclosures of personal data.

A. A PUBLIC RECORD OF GOVERNMENT PERSONAL DATA BANKS

Many of the privacy protection schemes we have examined impose a publicity requirement concerning the nature and existence of government-held personal data. Usually, government departments and agencies are required to publish an annual statement listing all personal data banks and certain characteristics of their design and operation. Under the Canadian scheme, these annual statements are published in a compendium which is made widely available to the public.

The reason for this requirement is perhaps self-evident. If the level of public anxiety concerning the personal data-gathering activities of government is to be reduced, it is essential that greater publicity be given to the extent and nature of these activities. The existence of "secret" personal data banks would do much to undermine public confidence that due recognition is being given to the individual right to privacy. More than this, such publicity may be seen as part of the larger concern, considered elsewhere in this report, that the affairs of government be open to public scrutiny. Public monitoring of these complex and extensive data-gathering practices can occur only if an authoritative and comprehensive source of information is provided to the public and is brought up to date at regular intervals.

A further reason for recommending the publication of an inventory of personal data banks is that such an inventory is a necessary prerequisite to the effective implementation of many of the other privacy protection mechanisms recommended in this report. For example, the effective exercise of the individual's right of access to government files containing personal information about him presupposes that it is possible for him to become aware of the nature of the data holdings maintained by government. Similarly, our recommendations relating to the supervision of the management of personal information systems assumes that the

data systems which will be the subject of this regulation must be identified in a systematic manner.

The Index of Federal Information Banks published by the Treasury Board of Canada (pursuant to the provisions of the Canadian Human Rights Act, Part IV) is a useful model. The index is published annually and, in accord with the statute, must "be made available throughout Canada in a manner commensurate with the principle that every individual is entitled to reasonable access thereto in order to be informed of the contents thereof"[7]. The index contains a notice relating to each personal information bank covered by the act, indicating in a general way the nature of the data bank, the nature of the personal information which it contains, and its principal uses.

In order to ensure uniformity in the reporting, we recommend that the following items of information be included for each data bank in an "Annual Systems Notice":

1. the name and location of the data bank;
2. the legal authorization for its establishment;
3. the types of information or data items maintained in the system;
4. the principal uses of the information and the categories of users to whom disclosures from the system are typically made;
5. the categories of individuals for whom records are maintained in the system;
6. the policies and practices applicable to the system with respect to storage, retrievability, access controls, retention and disposal of information maintained in the system;
7. the title, business address, and business telephone number of the official responsible for the operation of the system[8].

In addition to the annual systems notice, we recommend the publication of "new systems notices" containing similar information with respect to new information systems and substantial modifications of old systems. The new systems notices would be produced by a process of review in which the Data Protection Authority would grant its approval of the establishment of new systems or of changes in old systems. As will be indicated in

subsequent sections of this chapter, it is our view that the DPA should be responsible for reviewing the plans for such innovations and should exercise its judgment on the application of fair information practices principles to the design and operation of the systems in question.

In certain exceptional cases, it may be inappropriate to publish all of the items of information listed above with respect to a particular data bank. For example, a detailed description of the operation of a particular law enforcement data bank might reveal the nature of certain investigative techniques. In order to accommodate concerns of this kind, we recommend that systems notices not be required to contain information which would otherwise be exempt from access under the freedom of information law. In no case, however, should an institution be exempted from the general requirement of publishing a notice indicating the existence and general nature of each personal data bank which it maintains.

In summary, then, we recommend that annual systems notices and new systems notices, containing the items of information indicated above, be published on a regular basis and brought together in an annual compendium modelled on the Index of Federal Information Banks published by the Treasury Board of Cabinet pursuant to the provisions of the Canadian Human Rights Act, Part IV.

B. COLLECTION OF PERSONAL INFORMATION

As we have indicated earlier in this report, two different kinds of concerns arise with respect to the process of personal data collection. The first question, and in our view the most important, is whether the establishment of a particular data-gathering exercise is necessary or desirable. Obviously, the most effective method of privacy protection is simply to refrain from collecting the information in the first place. When a decision has been made to engage in such an exercise, however, a second group of questions must be considered. How can the data-gathering process be structured so as to minimize its intrusiveness on the privacy interests of the individual data subject? Should limitations be imposed on the methods of data gathering? Should certain information relating to the subsequent use of the material be communicated to the individual supplying information? In short, assuming that the gathering of data is necessary, what steps can be taken to reduce the intrusiveness of the process by which the information is obtained?

THE INITIAL DECISION TO GATHER DATA

In earlier chapters, we described the growth of government personal data-gathering practices -- a common feature in the recent history of modern industrial nations. It is unrealistic to suppose that it would be possible, through the enactment of privacy legislation, to return to a simpler and more private world. Nonetheless, we feel that steps should be taken to ensure that decisions to engage in the use of sophisticated information technologies should be informed by a clear perception of the privacy protection implications of projected increases in the government's personal data-gathering activities.

For this reason, we recommend that the proposed Data Protection Authority (DPA) should be given a mandate to comment on the privacy protection implications of new government programs involving the use of personal information data systems, and on changes within the administration of existing programs requiring the establishment of new systems or the significant alteration of existing systems. It is to be hoped that the DPA, having developed expertise in privacy protection problems, might be able to make useful suggestions for organizing administrative activity so as to reduce the need for intrusive information-gathering practices. With its comprehensive view of government data-gathering operations, the DPA could bring a useful perspective to the deliberations which should, in our view, precede the establishment of new programs involving increased use of personal data.

We wish to indicate clearly that this Commission is not opposed in principle to the use of sophisticated information technology by government. As we have said, the realization of the considerable benefits to society which may flow from the use of such technology should not be precluded on privacy protection grounds. A resolution of the complex and challenging problems facing governments may, from time to time, require the use of more rather than less information technology. Our concern is to ensure that in making a decision to exploit such technology, the privacy costs are properly weighed in the balance with other relevant considerations.

We envisage two situations in which the DPA could make a contribution of this kind. First, where proposed legislation establishes a program which will involve, in its proper administration, the creation of personal data information banks, the DPA should be invited to comment on the privacy protection implications of the proposed scheme. Ultimately, of course, the decision to adopt the legislative proposal is one to be made by the Legislative Assembly. It is our expectation, however, that a report from the DPA could be of assistance to the legislature in

its deliberations. (We note that a similar function is performed in New South Wales by the Privacy Committee[9].)

With respect to the operation of administrative activity authorized by statute, we recommend a somewhat different role for the DPA. In this context, we believe that it would be useful for the DPA to oversee the personal data-gathering activities of government departments and agencies with a view to ensuring that data collection does not exceed a level which has either been specifically authorized by statute or is necessary to accomplish the proper purposes and objectives of a particular program. This general standard of permissible data collection should be stated in the privacy protection legislation itself. On this point, the U.S. Privacy Act provides a useful model[10]. The role of the DPA, then, would be to approve the application of this standard to particular data-gathering exercises. A data system operated in accordance with directives of the DPA should be deemed to be in compliance with this statutory standard.

Under the U.S. legislation, the question of whether a particular agency is acting in compliance with the collection standard may ultimately be determined upon judicial review. It is our conclusion that after-the-fact review of this kind is not an attractive method for ensuring that the standard is observed in the operation of personal data systems. The prospect of dismantling expensive data-gathering systems in response to a subsequent determination that the collection is excessive is undesirable. In order to facilitate sound planning of personal data systems, we prefer enabling the DPA to make binding determinations when the system is first put into operation.

With respect to data-gathering activities which are already in operation at the time when DPA comes into existence, our proposals would operate in the following manner. Existing personal data banks would be subject to the general statutory standard; this might result, in certain instances, in a decision by the department or agency concerned to destroy some of the data in its existing collection. A department or agency which wished to do so could seek the opinion of the DPA as to whether its collection practices comply with the statutory standard. Alternatively, the DPA should be empowered to proceed on its own initiative to inspect an existing data bank and to require compliance with the statutory standard.

The adoption of a general standard of collection in the privacy protection statute will, we feel, respond to the public interest in ensuring that the gathering of personal data is properly tailored to the necessities of duly authorized government programs. The role of the DPA in elaborating and applying this

standard to specific data banks will reconcile the privacy interest and the need for effective and efficient planning and operation of government administrative activity.

REDUCING THE INTRUSIVENESS OF COLLECTION PRACTICES

Once it has been decided that the collection of personal information is necessary to the accomplishment of legitimate government objectives, consideration must be given to the means of collection. An individual's privacy might be threatened less by the actual information provided than by the methods of collecting and verifying that information. For example, individuals are likely to feel some discomfort when information is gathered without their knowledge or consent from friends and neighbours. Perceptions of privacy invasion may arise from a lack of knowledge of the purpose for which information is gathered and the terms and conditions on which it will be stored and disseminated. The sense that one has no control or involvement in governmental data collection or "dossier building" clearly undermines the individual's privacy interest.

We favour the adoption of statutory standards relating to collection coupled with a residual discretion conferred on the DPA to tailor the application of general principles to specific situations.

We recommend the adoption of the U.S. Privacy Act approach, which requires disclosure to the individual of certain material information about the data collection. It is our recommendation that, as a general rule, the individual from whom information is requested be informed in writing of:

1. the legal authority for the collection of the information;
2. the principal purpose or purposes for which the information is intended to be used;
3. whether disclosure is mandatory or voluntary, and the consequences of failure to provide the information;
4. such proposed use and dissemination of the information as can be reasonably anticipated;
5. the types of additional information and the sources to be used to verify the information;

6. the name, title and business telephone number of a public official who can answer any questions the individual may have with respect to the data collection;
7. whether the subject or some other individual will have access and correction rights to the information[11].

While communication of this information represents the ideal practice at the time of the solicitation of information, we appreciate that there are practical reasons for not imposing an obligation to communicate in this fashion every time information is solicited from an individual. Accordingly, we recommend that the DPA be empowered to establish standards indicating the manner and form in which such communications might take place. The Treasury Board guidelines indicate a variety of approved methods for communicating information of this kind[12]. Thus, the DPA might determine that in certain circumstances, the availability of brochures or the presence of other forms of notification may be adequate. As well, the DPA should be able to exempt information-gathering activities in which such notification is entirely unnecessary or impractical.

These recommendations, if implemented, should ensure that an informed decision to supply information can be made by the individual. Additional protection of the individual's privacy interests would be secured by ensuring that he himself is the source for the information in question. On this point, the U.S. act also provides a useful model. We favour including a provision worded similarly to section 552a(e)(2) which states that "to the greatest extent practicable" information should be collected directly from the "subject individual, when an adverse decision may result." Once again, we favour the conferral of discretion on the DPA to make binding determinations of the extent to which this standard applies to a particular situation.

RECOMMENDATIONS

Our recommendations with respect to the control of data collection practices are as follows:

1. The Data Protection Authority should have the responsibility to comment, where it deems it appropriate to do so, on the privacy protection implications of proposed legislative schemes or government programs.
2. A statutory duty should be imposed on government departments and agencies to collect only such personal information as is either expressly authorized by statute or

necessary to the proper administration of a lawfully authorized administrative activity.

3. The Data Protection Authority should have the power to:
 - a. make binding determinations as to whether a particular data collection meets the standards suggested in paragraph 2;
 - b. require a government department or agency to cease a collection practice which violates paragraph 2 and destroy collections of data gathered in violation of this standard.
4. A government department or agency engaged in the collection of personal information should inform the individual from whom the information is requested, in writing, of the following:
 - a. the legal authority for the collection of the information;
 - b. the principal purpose or purposes for which the information is intended to be used;
 - c. whether disclosure is mandatory or voluntary and the consequences of failure to provide the information;
 - d. such proposed use and dissemination of the information as can be reasonably anticipated;
 - e. the types of additional information and the sources to be used to verify the information;
 - f. the name, title and business telephone number of a public official who can answer any questions the individual may have with respect to the data collection;
 - g. whether the individual or some other person will have access and correction rights with respect to the information.
5. The Data Protection Authority should have the power to determine the extent and manner in which information required in paragraph 4 shall be communicated to the individual from whom the information is requested. It may, in appropriate circumstances, excuse the government

department or agency from engaging in communication of this kind.

6. To the extent practicable, a government department or agency should collect information directly from the data subject when an adverse determination may result.
7. The Data Protection Authority should have the power to excuse a government department or agency from compliance with paragraph 6.

C. STANDARDS FOR MAINTAINING THE INTEGRITY AND SECURITY OF DATA

The privacy protection schemes which we have examined typically impose duties on government departments and agencies with respect to the proper management of personal data banks. In essence, these provisions attempt to secure the integrity of the stored data and to protect the system from access or penetration by unauthorized persons. By "integrity of the data" we mean that the data is maintained with such accuracy, relevance, timeliness and completeness as is necessary to ensure fairness to the individual data subject. It is our view that such provisions are a desirable element of a privacy protection scheme. Once a decision to collect sensitive personal information has been made by government, a correlative duty of proper record maintenance and security should arise.

The central concern relating to the integrity of data arises when a determination of some kind is made, or an action is taken, based on the stored data relating to an individual. Both the individual and the department or agency have an interest in ensuring that decisions are made on the basis of accurate and complete information. It is our recommendation, therefore, that a statutory standard be imposed which will require the maintenance of data integrity so as to ensure fairness in the decision making relating to an individual. Again, we envisage the DPA making binding determinations of the application of this standard to specific information-gathering activities and imposing terms and conditions on new systems whose establishment is subject to its approval.

The gathering of intelligence data, which we have briefly described in Chapter 27, Section C, may constitute a legitimate exception to this general rule. The nature of intelligence gathering is such that the information obtained may be speculative or potentially unreliable. Nonetheless, because of its potential relevance to the prevention or detection of criminal activity, its retention may be desirable. However, we feel that such

information should be maintained in such a fashion as to signal its potential unreliability to all users[13].

In the interests of maintaining accurate, timely and complete information, personal data which is no longer needed by government should, as a general rule, be purged or destroyed. In Volume 2, Chapter 8, we described the records management program of the government of Ontario. This program attempts to ensure an orderly disposition of government records (including those containing personal data), leading ultimately either to their preservation by the Archives of Ontario or their destruction. An examination of schedules relating to personal record systems does not indicate, however, that privacy protection has been a predominant objective in the determination of time periods during which personal records may be maintained. Accordingly, it is our view that a general policy should be adopted to the effect that personal information no longer of use in the administrative and decision-making processes of government should be destroyed, subject to two limiting conditions. First, data ought not to be destroyed if its destruction could deprive the data subject of potential benefits to be derived from its storage. Thus, it should not be destroyed so soon after the determination of its utility as to render it difficult for data subjects to exercise their rights to seek access to their files. (With respect to this point, it may be noted that the Treasury Board of Canada guidelines indicate that personal data must be maintained for a minimum period of two years in order to ensure that it is not destroyed before the subject has had reasonable opportunity to conduct such an examination[14].) Similarly, the data ought to be maintained where future contact with the subject might be beneficial to him; for example, new medical treatment might have become available for an illness suffered by the subject. Second, data should not be destroyed where it is of potential value as a research resource or if it is material which, in the opinion of the provincial archivist, should be retained for its historical value. When data is to be retained for research or archival purposes, however, we believe that it would be useful to enable the DPA to impose terms and conditions on which it is to be stored and used until it is transferred to the Archives of Ontario.

The need for the establishment of safeguards to preserve the confidentiality and security of stored data has been referred to earlier in this report. It is our view that government departments and agencies should be subjected to a statutory duty, similar to that imposed by section(e)(10) of the U.S. Privacy Act, to

establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of

records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Again, we believe that it would be desirable to enable the DPA to give binding determinations as to the application of this standard to particular government data banks. In its examination of the experience under the U.S. Privacy Act, the PPSC noted a tendency for agencies to engage in overly expensive protective practices in order to ensure that they had met the standard imposed by the act. In our discussion of the privacy implications of the use of computer technology in Chapter 26, we noted the development of highly sophisticated security devices for computerized information systems. In order to facilitate sound and economical planning of security strategies, we believe that it would be useful to allow the DPA to establish general standards for security safeguards and to explicitly approve the security measures adopted with respect to a specific data bank. Determinations of the suitability of security arrangements would occur as a matter of course when the new data systems were approved by the DPA. With respect to existing systems, a determination could be made either at the invitation of the department or agency operating the system or upon the DPA's initiative where it was of the view that security safeguards pertaining to a particular system did not meet the statutory requirements.

RECOMMENDATIONS

1. Record keepers should maintain all records used in making a determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual concerned.
2. The Data Protection Authority should be empowered to make final determinations of the application of the standards set forth in paragraph 1 to specific data-gathering systems.
3. The gathering of intelligence information for law enforcement purposes should constitute the exception to the general standards set out in paragraph 1; provided, however, that the information is stored in such a way as to signal its unreliability to users.
4. The duty should be imposed to destroy personal data no longer useful for the accomplishment of the objectives

for which it was originally collected, unless destruction would potentially deprive the data subject of some benefit resulting from its storage or unless the data is to be stored, on terms or conditions approved by the DPA, for use as a research resource or for ultimate transfer to the Archives of Ontario as data of historical value.

5. Record keepers should establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats to their security or integrity.
6. The DPA should make final determinations of the applications of the standards set forth in paragraph 5 to specific data systems.

D. CONTROLLING TRANSFERS OF DATA

Perhaps the major concern arising from the collection of substantial amounts of personal data by government is the fear that information collected for one purpose may be used, to the disadvantage of the data subject, for quite another purpose. It is no doubt for this reason that Alan F. Westin defines "informational privacy" as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others[15]." When sensitive personal information has been collected by government, the informational privacy interest is further violated if that information is transferred from one agency to another, or if the collecting agency uses the data for a purpose other than that for which it was collected. For this reason, a careful consideration of the problematic aspects of "transfers of personal information" is an important element in our review of privacy protection issues. Our examination of current information practices of the government of Ontario indicates that this is a legitimate area for concern and suggests that practices inconsistent with fair information principles do occur from time to time[16].

The adoption of controls over data transfers is a theme addressed in most discussions of the informational privacy issue. For example, the report of the U.S. Department of Health, Education and Welfare sets forth this proposition:

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent[17].

As we have seen, such controls are typically found in legislated privacy protection schemes. The European approach to this problem, as a general rule, involves the promulgation of detailed codes of transfers specifically tailored to each data bank subject to the data protection scheme. In Sweden, for example, the licence for a particular data keeper contains, among other things, restrictions on the data keeper's ability to transfer the data. The control mechanism can thus be used somewhat flexibly to meet unusual needs or problems associated with a particular data bank.

A second approach taken to this problem is exemplified in both U.S. federal and state statutes and in the Canadian Human Rights Act. Typically, these schemes provide that no transfer shall be made unless the data subject consents or unless the transfer fits into a category exempt from the "no-transfer" rule. Although such schemes lack the flexibility of the European model, the expression of the no-transfer rule in the statute (and the exemptions) does have the virtue of giving a clear statutory basis to a principle which we feel is central to a privacy protection scheme. To the extent that the policy can be stated in general terms, we think it desirable to embody the no-transfer rule and its exemptions in the statute itself. Including the rule in the statute will ensure that an authoritative statement of the general policy covering this matter is readily accessible to all interested citizens.

Further, it is our view that the no-transfer rule should, prima facie, apply to all data transfers so that individuals may be assured that the rule and its exceptions set forth a complete code governing the transfer of data. As we have pointed out, Part IV of the Canadian Human Rights Act does not adopt this approach, and we have expressed the view that the act's provisions do not offer a sufficiently comprehensive solution to the transfer problem.

It is evident, however, that it would be both impractical and undesirable to adopt an absolute principle that information concerning individuals cannot be transferred from one government agency to another (or, in appropriate cases, from government agencies to individuals or institutions outside government). How can the necessary exemptions to the general principle of no transfer be fashioned so as not to reduce unacceptably the value of privacy protection embodied in the no-transfer principle?

FOI REQUESTS

One obvious exemption to the no-transfer rule relates to access to personal data granted pursuant to a freedom of information

request. In our freedom of information recommendations, we have attempted to devise a set of principles which would strike an appropriate balance between the public's right to know and the need to protect individual privacy. For example, personal data which would be instrumental in furthering valuable research should be made available, subject to appropriate safeguards. Assuming that a proper judgment has been made of the need for allowing third parties access to personal information in pursuit of freedom of information objectives, transfer pursuant to the freedom of information provisions must count as a legitimate exemption to the no-transfer rule.

ROUTINE OR DERIVATIVE USES

A much more difficult issue arises with respect to the proper characterization and control of what have been referred to in the United States as "routine" uses, and in Canada as "derivative" uses. Essentially, these are uses compatible with or necessarily incidental to the purpose for which the information was gathered in the first place. A typical example of a routine use is disclosure of personnel and other records of an operating branch to the payroll division of a personnel branch in order to facilitate the completion of a payroll. There may also be situations in which disclosure from one level of government to another (or, indeed, to a member of the public) is obviously compatible with the purpose for which the information was gathered. Thus, the transfer of income tax data from the federal to the provincial government in order to facilitate tax-sharing schemes is necessary. Information about an individual seeking a job with the government might be disclosed to a person whose name was supplied by the data subject as an employment reference. How can compatible uses such as these be identified and permitted without opening the door to wholesale transfers of personal data which would violate the general principle underlying the no-transfer rule?

The U.S. Privacy Act addresses the problem in the following two exemptions:

552a(b) Conditions of disclosure. -- No agency shall disclose any record...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be --

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;...

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e) (4)(D) of this section;...

Routine uses are, in effect, broken down into categories. In subsection (1), the problem of routine use for internal agency purposes is addressed by permitting agency employees to have access if they have a "need to know." For other routine uses, reference must be made to subsection (3), which brings into play the concept of "routine use," specifically defined in subsection (a)(7) of the act to mean "the use of [a] record for a purpose which is compatible with the purpose for which it was collected." Subsection (3) further limits the concept of routine use to those exemptions which have been described under subsection (e)(4)(D), which is the "system notice" provision requiring publication of a list of the routine use of each record system in the Federal Register. As we noted in our discussion of the U.S. act[18], routine uses must be disclosed in the Privacy Act "statements" which must be given to data subjects when information is gathered from them.

The PPSC Report makes a number of criticisms of these provisions. The internal-use "need to know" provision is criticized on the basis that in a large agency, such as HEW, transfer of data among agency personnel may well violate the basic premise of the no-transfer rule -- information gathered for one purpose ought not to be used for another without the knowledge or consent of the data subject. Accordingly, the PPSC recommended that the internal use of data be permitted only in accordance with the "routine use" test of subsection (3)[19].

The PPSC also feared significant deficiencies in the operation of the "routine use" test itself. Agencies have taken a very broad view of the discretion conferred upon them by the "routine use" concept and have described in the Federal Register routine uses which could not conceivably be considered as "compatible" with the purpose for which the information was collected[20]. The U.S. Commission on Federal Paperwork (CFP) also notes this phenomenon and cites the practice of many agencies of sharing medical information with law enforcement agencies[21].

The PPSC recommends that the concept of "routine use" be refined so as to ensure that the so-called "compatible" uses are consistent with the reasonable expectations under which the subject originally submitted the information. The proposed draft put forward by the PPSC is as follows:

The term "routine use" means the use of disclosure of an individually identifiable record for a purpose which is:

- (a) compatible with the purpose for which the information in the record was collected or obtained, and
 - (b) consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained[22];
- ...

The PPSC's revised version of the internal-use disclosure provision then tightens the concept of "compatible" use for internal purposes:

- (3) To those officers and employees of the agency who have a need for the record in the performance of their duties, provided, however, that such disclosure is:
 - (a) necessary and proper for the performance of the agency's own mission and functions, and
 - (b) a routine use as defined by subsection (a)(9) of this section[23].

As far as routine uses for individuals outside government are concerned, the PPSC recommends not only that there must be a "routine use" within the meaning of its new definition, but also that it must be certified to be such by an official designated under the provisions of its revised act as the agency official responsible for the agency's compliance with the Privacy Act.

Our discussion of the implementation of Part IV of the Canadian Human Rights Act[24] indicated that a similarly restrictive view of the concept of "derivative use" has been developed in the Treasury Board guidelines. Our view is that while an exemption for "routine" or "derivative" uses is a necessary element in the scheme, the concept should be restrictively defined along the lines proposed by the PPSC in order to prevent this device from being used to undermine the protection afforded by the "no-transfer" rule.

A further difficulty identified by the PPSC relates to the integration of the "routine use" concept with existing statutory provisions which confer discretion on an agency or an official to disclose identifiable personal data. Although the Privacy Act provisions do not contain an explicit exemption for transfers permitted under other statutory provisions, many agencies have apparently interpreted such provisions as establishing a basis for "routine uses." The PPSC views this as an abuse of the routine-use concept, especially where the statutory provision in question simply "authorizes" the agency to disclose but does not "require"

it to do so. The solution proposed by the PPSC is to develop a new concept of "collateral use," permitting disclosures under other statutory provisions only if the provision in question establishes specific criteria for the use or disclosure of specific types of information[25].

DATA SUBJECT CONSENT

Transfers of information to which the data subject consents constitute an obvious third exception to the general rule. However, special care must be taken to ensure that such consents are genuinely voluntary and informed. The U.S. Commission on Federal Paperwork (CFP) noted in its study that agencies have attempted to circumvent the no-transfer restrictions by employing blanket consent forms[26]. Agencies have apparently adopted the practice of obtaining written consents, often when the information is initially collected, authorizing wholesale disclosure of personal information for a variety of stated purposes. The CFP questioned whether such consents can fairly be considered to be "informed" and "voluntary" inasmuch as they are often given as a prerequisite to obtaining some benefit, privilege or other entitlement.

The solution proposed by the CFP is simply to permit disclosure only in cases where specific written request or authorization has been given by the subject, and not where a general open consent to disclosure has been obtained. Further, the CFP recommends that no agency should require an individual to execute a general consent of this kind, nor should the agency be permitted to deny an individual any right, privilege or benefit because of his failure to do so.

Under the Canadian scheme, the matter of informed and voluntary consent is regulated to some extent in the Treasury Board guidelines[27]. In brief, the guidelines require that when a consent is sought, the non-derivative use should be precisely identified, the data subject should be given an opportunity to positively indicate his consent, and he should be advised that any refusal to consent for non-derivative use will not result in an adverse decision in conjunction with the particular purpose being served by the collection of information. Although the agency is permitted to seek consent either at the time of collection or subsequently, an attempt is thus made to control the format of the request for consent in order to ensure that it is informed and voluntary.

We agree that qualifications of this kind should be imposed on the "consent" exemption to the no-transfer rule.

LAW ENFORCEMENT

Access to personal data for law enforcement purposes is obviously a matter of considerable sensitivity. The granting of wholesale access to government-held personal files for such purposes would simply defeat the objectives of the no-transfer rule. Some evidence of public, and indeed, governmental feeling on this matter may be drawn from the circumstances surrounding the establishment in 1978 of the Royal Commission of Inquiry into the Confidentiality of Health Records (the Krever Commission). It will be recalled that rumours of Ontario Provincial Police access to the files of the Ontario Hospital Insurance Plan led to much public discussion, and ultimately to the commission's establishment.

On the other hand, it is equally evident that some accommodation of the public interest in the enforcement of law must be made in schemes of this kind. It is obvious that law enforcement authorities must have access to personal data in order to enforce the laws under which the data was originally collected. The more difficult issue is whether, and in what manner, access to personal data should be granted for law enforcement activities unrelated to the original purpose of collection of the data. No doubt, it might be of great assistance to law enforcement authorities to have complete and unrestricted access to all government files. The detection of crime, and in particular, various forms of fraud, might be substantially enhanced by allowing a complete integration of all government data banks. In our view, however, the possible benefits from such unrestrained access are substantially outweighed by the intrusiveness of such a scheme and the resulting injury to the privacy values we have identified in this report as worthy of preservation.

The well-established mechanisms of our legal process attempt to strike a balance between the rights of the subject and the public interest in access to information which will lead to the conviction of those who have committed criminal or quasi-criminal offences. The traditional mechanisms of the search warrant or other judicial orders are the proper means for gaining access to personal information in government files. Just as one would not gain access to a person's home without a properly issued search warrant[28], so too, we believe, access should not be granted to sensitive data in one's welfare or medical files without proper legal process. The effect of this requirement is to ensure that a judicial officer will have to be satisfied that the granting of access is reasonable in the circumstances and is related to a specific investigation of a particular offence.

The Canadian Human Rights Act, Part IV, appears to adopt a similar approach. While access to information for enforcement of the statute under which it was collected would be considered a proper "derivative" use, the granting of access for other law enforcement purposes would be a "non-derivative," "administrative" use and is therefore not permitted without the consent of the subject. Disclosure can be made, however, where the non-derivative use is authorized by or is pursuant to law. Accordingly, access could be obtained if proper legal process (for example, in the form of a search warrant) was observed.

The U.S. Privacy Act has adopted a rather different solution to the law enforcement problem. The act provides[29] in exemption 7 that access will be given if the law enforcement activity is authorized by law, and if the head of the requesting agency has specified in writing the particular portion of the record desired and the law enforcement activity for which it is sought. The PPSC report indicates, however, that this provision has been virtually ignored by agencies undertaking investigations and that the agencies have adopted a practice of defining "routine use" in such a way as to permit law enforcement authorities broad access. Thus, a typical "routine use" definition reported by the PPSC[30] provides that "a record may be disseminated to a federal, state, local, foreign or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency or to assist in general civil matters or cases." Such definitions of routine use are evidently designed to evade the clear requirements of exemption 7.

The solution proposed by the PPSC is, as indicated above, to restrictively define the concept of "routine use" in such a way as to make it clear that broad law enforcement access is not within its scope. Law enforcement agencies are thus left to rely on exemption 7 or on judicial process as vehicles for access to material. Presumably, however, access given for the purpose of enforcing the statute under which the information was initially collected would fit within the new definition of "routine use" and would not require either compliance with exemption 7 or judicial process.

Although our general conclusion is that the approach taken in exemption 7 does not adequately protect personal privacy, there is one attractive feature to this provision. The requirement of written approval from the agency head will ensure that a record is kept of such transfers, which may ultimately be of assistance in reviewing the effectiveness of the protections afforded by the act. We would recommend that recording systems be developed,

where feasible, to permit subsequent scrutiny of law enforcement use of personal data in government files.

One final issue must be considered. The account of law enforcement information systems in Ontario published in a Commission research paper indicates the existence of information-sharing practices among federal, provincial, municipal, and even foreign law enforcement agencies[31]. Clearly, such cooperative efforts are instrumental in the apprehension of suspected criminals, and it would be unwise, in our view, to preclude information exchanges for that purpose. Such information will not normally be submitted voluntarily by the data subject in the first place. Information gathered in the course of an investigative activity will most commonly be shared in order to secure assistance from other law enforcement officials who may have an opportunity to apprehend suspected parties. Accordingly, we recommend that such exchanges be exempt from the no-transfer rule. We do feel, however, that exchanges of law enforcement information, especially with foreign law enforcement agencies, is a matter which should be the subject of clear understandings, properly committed to written agreements, legislation or treaties which would be subject to scrutiny and evaluation by legislators and interested members of the public.

HEALTH AND SAFETY OF AN INDIVIDUAL

Access to personal data held by a government institution should be granted to another government department or agency or to an individual where it may be instrumental in preserving the health or safety of an individual from serious risk, whether the individual in peril is the data subject or a third party. This principle is reflected elsewhere in our proposals[32] and should be adopted as an exception to the no-transfer rule.

LOCATION OF NEXT OF KIN

Discussions with Canadian federal officials responsible for implementation of the Canadian Human Rights Act privacy provisions show that the act appears to unnecessarily restrict access to personal data for the purpose of locating the next of kin or friends of an individual who is injured, ill or deceased. We recommend the adoption of an exemption to facilitate such contact in compassionate circumstances.

MEMBERS OF THE LEGISLATIVE ASSEMBLY

Access to personal data appears to be available to the Legislative Assembly or its committees under the pertinent provisions of the Legislative Assembly Act[33]. We understand that access is commonly given to members of the legislature who are seeking redress of grievances brought to them by their constituents. This practice, potentially of benefit to the constituents involved, should be a permitted exemption from the no-transfer rule, provided that it is clearly stipulated that the member in question must be acting at the request of a constituent or, where the constituent is incapacitated, by a relative or legal representative of the constituent.

AUDITING/DISPUTE RESOLUTION

Access to personal data should also be permitted to certain government agencies or public officials in the public interest to permit the auditing of government programs or to facilitate dispute resolution on behalf of aggrieved individuals. Thus, exemptions should be provided to permit transfers to the Provincial Auditor and the Ombudsman, and to agencies such as the Data Protection Authority, the Director of Fair Information Practices, and the Fair Information Practices Tribunal, whose establishment is recommended in this report. In appropriate cases, it may be necessary to grant access to federal officials in order to facilitate auditing of programs jointly financed by the federal and provincial government.

ARCHIVES OF ONTARIO AND STATISTICS CANADA

Transfers of identifiable data for archival, research or statistical purposes to the Archives of Ontario and to Statistics Canada constitute an obvious exception to the no-transfer rule.

RECOMMENDATIONS

In conclusion, then, we make the following recommendations with respect to the control of transfers of identifiable personal data:

1. No disclosure or transfer of identifiable personal data should be made unless the disclosure comes within one of the following exceptional cases:
 - a. disclosure under the freedom of information provisions;

- b. a "routine" use as defined by the PPSC, i.e., a use for a purpose which is:
 - i. compatible with the purpose for which the information in the record was collected or obtained, and
 - ii. consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected or obtained, and
 - iii. where disclosure is made to an officer or employee of the agency who has need for the record in the performance of his duties, access may be granted where it is necessary and proper for the performance of the agency's own mission and functions;
- c. disclosure for a "collateral use" as defined by the PPSC, i.e., disclosure pursuant to statutory provisions, provided that such provisions establish specific criteria for the use or disclosure of such information;
- d. disclosure by a law enforcement agency to another law enforcement agency in Canada or to a law enforcement agency in a foreign country, provided that in the latter case the disclosure is made pursuant to a written agreement, a treaty or a legislative authority;
- e. disclosure to a person pursuant to his showing of compelling circumstances affecting the health and safety of an individual;
- f. in compassionate circumstances, disclosure to facilitate contact with the next of kin, or a friend, of an individual who is injured, ill or deceased;
- g. disclosure to a member of the legislative assembly who has been authorized by a constituent to make an inquiry on his behalf or, where the constituent is incapacitated, has been authorized by a relative or legal representative of the constituent;
- h. to the Provincial Auditor;
- i. to the Ombudsman of Ontario;

- j. to the Data Protection Authority;
- k. to the Director of Fair Information Practices;
- l. to the Fair Information Practices Tribunal;
- m. to the federal government in order to facilitate the auditing of shared-cost programs;
- n. to the Archives of Ontario;
- o. to Statistics Canada.

E. SUBJECT ACCESS AND CORRECTION RIGHTS

Implementation of the proposals advanced thus far in this chapter would do much to redress the imbalance in control over personal information which currently exists between the governmental institutions which gather the information and the individual data subjects who supply it to them. In essence, we have recommended measures which are designed to eliminate unnecessary collection of personal information and to ensure that such personal information as is collected is maintained and used in a manner consistent with the privacy interests of the individual. And yet, as the federal Canadian task force observed in 1972, "no matter how much external assistance may be provided to redress the balance by controlling the activities of data banks, the individual remains the protagonist in the drama. Only an individual can determine whether particular types of information are of importance to himself or herself and therefore worth the effort required to ensure their accuracy or to restrict their dissemination"[34]. It is for this reason, presumably, that nearly all of the commentators and study groups who have examined these problems stress the need for subject access and correction rights as a central element in privacy protection schemes. Virtually every privacy protection law this Commission has examined facilitates access by the data subject to his file and provides him with an opportunity to dispute the accuracy of the records contained therein.

The HEW report articulated in considerable detail the nature of the rights which should be conferred upon the individual. The report recommended that an organization maintaining administrative automated personal data systems should:

1. inform an individual, upon his request, whether he is the subject of data in the system, and, if so, make such data fully available to the individual, upon his request, in a form comprehensible to him;

2. inform an individual, upon his request, about the uses made of data about him, including the identity of all persons and organizations involved and their relationships with the system;
3. maintain procedures that (i) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; (ii) permit data to be corrected or amended when the individual to whom they pertain so requests; and (iii) assure, when there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in the subsequent disclosure or dissemination of the disputed data[35].

Provisions establishing mechanisms for accomplishing these objectives are a common feature of the U.S. federal and state privacy protection laws.

Similarly, the Canadian Human Rights Act, Part IV, embodies these principles in the following terms in section 52(1):

52(1) In furtherance of the principle enunciated in paragraph 2(b) that the privacy of individuals and their right of access to records containing personal information concerning them for any purpose including the purpose of ensuring accuracy and completeness, should be protected to the greatest extent consistent with the public interest, every individual is entitled to

(a) ascertain what records, concerning that individual that are used for administrative purposes are contained in federal information banks named or otherwise identified in the publication referred to in subsection 51(1);

(b) ascertain the uses to which such records have been put since the coming into force of this Part;

(c) examine each such record or a copy thereof whether or not that individual provided all or any of the information contained in the record;

(d) request correction of the contents of any such record where that individual believes there is an error or omission therein; and

(e) require a notation on any such record of a requested correction therein where the contents of such record are not amended to reflect the requested correction.

The procedures to be employed in giving effect to these access and correctional rights are set forth in considerable detail in the Treasury Board guidelines[36].

As we have indicated elsewhere in this report, subject access and correction rights have been granted to the subjects of credit reports[37] and to students enrolled in the public educational system[38]. Subject to certain exemptions which we will discuss later, we propose that these rights be extended to all individuals about whom personal information is stored by governmental institutions in the province of Ontario.

The experience of other jurisdictions which have granted access and correction rights with respect to government-held personal records indicates that questions concerning the nature and extent of such rights will arise.

- . To what kinds of records should access and correction rights pertain?
- . What is the nature of the access right?
- . What is the nature of the individual's right to correct the record?
- . What should be the extent of the governmental duty to propagate corrected information?
- . What kinds of records should be exempt from the subject access correction scheme?
- . What fees should be chargeable for the processing of requests?
- . What time limits, if any, should be imposed for the processing of access and correction requests?
- . In what form should denial of access and correction requests be made?

We will consider each of these issues in turn.

TO WHAT KINDS OF RECORDS SHOULD ACCESS AND CORRECTION RIGHTS PERTAIN?

In our freedom of information proposals, we recommended that individuals be granted a general right of access to government documents; provided, of course, that its contents do not bring the document within a category of information which is exempt from the general principle of public access. It is our recommendation that a similarly broad right of access and a corresponding right of correction be given to individuals with respect to records containing personal information. Inasmuch as the nature of the access right given to the individual data subject will differ in certain respects from the general right of access set forth in our freedom of information proposals, it is necessary to define more precisely "a government document containing personal information."

The statutory schemes which we have examined contain a number of definitions of "personal records"; we believe that the concept is most straightforwardly expressed in the Canadian Human Rights Act. The act defines the term "record" to mean "an item, collection or grouping of personal information recorded in any form," and further defines "personal information" as "information respecting an individual if that information contains the individual's name or if the individual's identity is readily ascertainable from that information"[39]. It is to this kind of record, we suggest, that access and correction rights should apply.

Our freedom of information proposals limit the right of general access to the extent that the duty to provide government records obtains only in cases where the record can, with reasonable effort, be located by the personnel of the government institution concerned. We propose a similar limitation on the access and correction rights pertaining to records containing personal information. Where the information is stored in an organized fashion and is accessible on the basis of the individual's name or some other identifying device, it is evident that the record may easily be retrieved. Most access and correction requests will probably relate to information of this kind. In the typical case, the data subject will be interested in the contents of a file relating to a determination to be made concerning him. If this is so, it is likely that the institution involved has a systematic method of organizing such files. Alternatively, the data subject may be interested in the contents of the file on the basis of a reading of the index of personal data systems. Again, the data will be stored in an organized fashion and retrieval will not be difficult. There may be other situations, however, in which personal information is not stored in this manner. We see no reason for not allowing subject access in such situations, as long as the data subject can give instructions which can, with

reasonable diligence on the part of the personnel of the government institution, enable the record to be found.

Before leaving this matter, we should indicate that the Canadian Human Rights Act, Part IV, and the U.S. Privacy Act of 1974 approach this matter in a different way. In essence, both these schemes provide access and correction rights only with respect to personal data which is systematically stored in a data bank. The Canadian act further limits the access and correction rights to data banks which are used for "administrative purposes," which is to say, "in a decision-making process which relates directly to the individual"[40]. The limitation of these rights to records stored in data banks is imposed, presumably, for purposes of administrative convenience. It is our view, however, that the need for administrative convenience is sufficiently met by our recommendation that personal records be made available only where they can, with reasonable effort, be located.

The further limitation expressed in the Canadian act with respect to records used in a decision-making process, however, raises a more difficult issue. We assume that the theory underlying the Canadian provisions is that the individual data subject's privacy interest is more compelling where the data is potentially of relevance to a determination which will be made concerning him by the government institution holding the record. Although there is evident merit in this position, it is our view that the anxiety that individuals may feel as a result of the presence of inaccurate information in government files will not be assuaged by the realization that the government has no immediate reason to make a decision affecting the individual on the basis of that information. The individual may well feel that he wants government records concerning him to be completely accurate, even if there is no immediate prospect of any decision or action being based upon them. It seems very likely that the majority of access and correction requests would relate to information contained in administrative data banks. Nonetheless, we are persuaded that the statutory rights of the data subject should not be so circumscribed. It is of interest to note that the PPSC has recommended that the U.S. Privacy Act be amended so as to permit a similarly broad right of access and correction[41].

THE NATURE OF THE ACCESS RIGHT

In the ordinary case, access to data should be granted to the subject by enabling him to see and make a copy of the records that are available to him under these provisions. It is quite conceivable, however, that the information might be stored in such a fashion that it would be incomprehensible to the individual if it were simply reproduced in the same form. This would be the case,

for example, where the data is stored in machine-readable computer language. In such situations, the information should be provided in a form which is comprehensible to the applicant. Further, an applicant who feels that he may have difficulty in understanding the significance of the record should be permitted to authorize another individual to have access to his files on his behalf.

Where practical, the information should be communicated so as to make clear the general terms and conditions under which the governmental institution maintains and uses the data in question[42]. The Treasury Board guidelines suggest that this may be effected by directing the individual to the index or by communicating this information separately at the time of the access request[43].

THE NATURE OF THE CORRECTION RIGHT

The ability to correct information contained in a personal record will be of great importance to an individual who discovers that an agency is in default of its duty to maintain accurate, timely and complete records. In this way, the individual will be able to exercise some control over the kinds of records that are maintained about him and over the veracity of information gathered from third-party sources.

Although the report refers to the individual's "right" to correct a file, we do not feel that this right should be considered absolute. Thus, although we recommend rights of appeal with respect to correction requests, agencies should not be under an absolute duty to undertake investigations with a view to correcting records in response to each and every correction request. The privacy protection schemes which we have examined adopt what we feel to be appropriate mechanisms for permitting the individual to file a statement of disagreement in situations where the governmental institution does not wish to alter its record. In particular cases, an elaborate inquiry to determine the truth of the point in dispute may incur an expense which the institution quite reasonably does not wish to bear. Moreover, the precise criteria for determining whether a particular item of information is accurate or complete or relevant to the purpose for which it is kept may be a matter on which the institution and the individual data subject have reasonable differences of opinion.

If the request for correction is denied, the individual must be permitted to file a statement indicating the nature of his disagreement. We recommend that an individual who has been denied a requested correction may exercise rights of appeal to an independent tribunal[44]. The tribunal, in turn, could order

correction of the file or simply leave the individual to exercise his right to file a statement of disagreement.

THE DUTY TO PROPAGATE CORRECTIONS

An individual data subject who has identified an inaccuracy in his personal record will wish to be assured that the correct information (or his statement of protest) will find its way into all other government-held records which contain this item of information. Thus, for example, if a criminal record of some kind has been falsely attributed to the subject, he will wish to ensure that other users of the criminal record file are advised of the error. For this reason, the U.S. Privacy Act embodies a requirement that agencies engage in a "propagation" of corrections and statements of protest[45].

We are in general agreement with the notion that a duty of this kind should be imposed. Care must be taken, however, to fashion a duty to propagate which meets the needs of the data subject but does not create unduly burdensome administrative responsibilities. The most obvious requirement to impose on governmental institutions is that all future disseminations of information from the corrected file be based on the corrected information or, in a case where a statement of protest has been filed, signal the existence and nature of the protest. Second, there is evidently a strong argument for imposing an obligation to forward corrections to third parties to whom the information had previously been disclosed, provided that the identity of the third party is known to the agency. These are, in fact, the burdens which have been expressly imposed on U.S. federal agencies by the Privacy Act of 1974.

In reviewing the implementation of this principle, the PPSC identified two further categories of potential recipients for corrections and statements of protest. First, the original sources of the information should be informed of the error in question. Second, an attempt should be made to communicate with prior recipients of information within the agency. Thus, according to the PPSC, if incorrect criminal record information was communicated to another record system within the agency before the error is discovered, an attempt should be made to communicate the corrected information to that agency.

The PPSC did not recommend the establishment of an absolute duty to contact all sources and all prior recipients of incorrect information. It was the commission's view that it would be satisfactory to impose a duty to take "reasonable affirmative steps" to furnish corrected information to sources and prior recipients with whom the agency had contact within a reasonable

period of time prior to the exercise of the correction right. Further, the PPSC essentially limited the duty to a requirement to communicate with sources and prior recipients within government. The commission did recommend, however, that the data subject should have a right to require the record-holding agency to communicate with other sources and prior recipients named by the data subject[46].

Although we are in general agreement with the thrust of the PPSC proposals, we believe that this is a sufficiently subtle problem that it may be appropriate to confer on the Data Protection Authority (DPA) a discretion to determine appropriate solutions for particular situations. We therefore favour the imposition of a statutory duty to communicate corrections and statements of disagreements to all future recipients of data. With respect to prior recipients and sources of information, however, we believe that the DPA should develop and implement standards imposing duties to communicate corrections where fairness to the individual requires it.

In Section G of this chapter, we make certain recommendations with respect to the maintenance of a record of uses and disclosures made of data containing personal information. We suggest that the DPA be assigned the task of approving the administrative arrangements under which a particular record-keeping system complies with this obligation. In establishing such accounting mechanisms, the efficient propagation of corrections to governmental record keepers should be facilitated to the extent that it is practicable to do so.

WHAT KINDS OF RECORDS SHOULD BE EXEMPT FROM THE SUBJECT ACCESS AND CORRECTION SCHEME?

It is evident that the individual's interest in having full and complete access to all government files containing information about him must yield, on occasion, to the public interest in permitting the government to maintain confidentiality with respect to certain kinds of files. Thus, there must be some exemptions to the general principle of allowing data subjects access and correction rights. We here return to a problem which required much careful consideration in the context of our freedom of information proposals. Before turning to the exemptions which we feel are appropriate in the present context, it will be useful to indicate, in a general way, the relationship between information requests under freedom of information schemes and subject access and correction rights under a privacy protection law.

The U.S. experience under the federal Freedom of Information Act (FOIA) and the Privacy Act of 1974 has provided an interesting

and illuminating illustration of the relationship between these two different types of schemes. As the report of the PPSC indicates, U.S. experience shows that care must be taken to ensure that the rights of access conferred on individuals by these two laws are properly integrated.

The potential conflicts between the two schemes are shown by the fact that the Freedom of Information Act has the effect of providing rights of subject access. An individual who wishes to have access to a government record containing personal information may elect to seek such access under the Freedom of Information Act. Such a record would not constitute "unwarranted invasion" of the requester's own privacy. Accordingly, provided that no other exemption in the FOIA applies, access to the personal record can be obtained. Alternatively, of course, the individual might wish to seek access to his file under the Privacy Act of 1974. If the individual wished to exercise rights of correction, it would be necessary to proceed under the provisions of the Privacy Act.

A particularly astute requester seeking access to sensitive personal information would engage in a careful comparison of the exemptions from access contained in the two acts. As we noted earlier, the Privacy Act exempts those "systems of records" relating to certain kinds of law enforcement and intelligence-gathering activity. Inasmuch as the FOIA scheme does not permit the exemption of entire systems of records in this way, an individual seeking access to such material would prefer to exercise his rights under the FOIA. This practice has indeed occurred on several occasions, and there is some irony in the fact that data subjects have been able to obtain greater access to their files under the FOIA than they could obtain under the Privacy Act. One of the lessons to be drawn from the U.S. experience, then, is that the freedom of information exemptions should be properly integrated with the exemptions to the subject access and correction rights proposals. In addition, we see that the exemptions in a subject access and correction scheme will not necessarily be identical to those in a freedom of information scheme. There are three reasons for this. First, some of the exemptions to the FOIA are simply inapplicable to personal records.

It is difficult to conceive of a situation in which personal information requested by a data subject could constitute a "trade secret" of the kind protected by the U.S. FOIA commercial information exemption. Second, the claim of a data subject in obtaining access to personal information may weigh more heavily than the claim of a merely curious observer who wishes to have general access to government files. Thus, the exemptions from the general rule of access under the freedom of information scheme may be too sweeping when applied to the access rights of a data subject. The PPSC report cites an example relating to the exemption of what

might be termed "deliberative" materials[47]. Although this exemption is established, as a general rule, under the FOIA[48] there is no equivalent exemption to the subject access scheme of the Privacy Act. It was the view of the PPSC that individuals who sought access to their files under the FOIA were being unfairly deprived of access on the basis of the deliberative materials exemption. In short, while deliberative materials may, as a general rule, be exempt under a freedom of information scheme, deliberative materials affecting the individual ought to be available to the data subject when he exercises his access rights.

A third reason for not simply adopting freedom of information exemptions in a subject access and correction scheme is that the freedom of information exemptions are not likely to meet the conflict of interest which may arise on an individual's application for access. The U.S. FOIA generally exempts information the disclosure of which would constitute a "clearly unwarranted invasion of privacy." The effect of this exemption is to exclude from general public access vast quantities of government records containing personal information. The effect of allowing access to this material by the data subjects themselves creates a need for exemptions which may not have been considered necessary in the context of the general freedom of information scheme. Thus, exemptions relating to some kinds of medical and correctional records are a common feature of privacy protection schemes. They are not found in the U.S. FOIA.

In summary, then, three important observations can be made on the basis of an examination of the U.S. experience dealing with subject access problems under both the FOIA and the Privacy Act. First, it would be useful to duplicate some of the subject access exemptions in freedom of information legislation. Second, it would not be desirable simply to transport all of the freedom of information exemptions to the subject-access context. Some, but not all, of the freedom of information exemptions set appropriate limits to the rights of the data subject. Third, it may be necessary to fashion exemptions from the general rule of data subject access which would not be found in the freedom of information exemptions.

Similar lessons could be drawn from a comparison of the exempting provisions of the Canadian Human Rights Act, Part IV, with the exempting provisions of the proposed federal freedom of information law, Bill C-15[49]. The exemptions in the two different schemes differ in much the same way as do the U.S. Freedom of Information Act and Privacy Act. Care must be taken to ensure that information unavailable to a data subject under the privacy scheme is not available to him under the freedom of information scheme.

Before recommending particular exemptions to subject access and correction rights, we wish to draw attention to three matters of general significance relating to the design of exemptions of this kind:

- a. the exemption should be "permissive" rather than "mandatory";
- b. a principle of "segregability" should apply;
- c. the exemption should pertain to particular items of information rather than to entire data systems.

Our recommendations on these points are consistent with our views of similar matters in the context of our freedom of information proposals. Nonetheless, it may be useful to reiterate the bases for each of these conclusions.

Exemptions should be permissive rather than mandatory

In our freedom of information proposals, we noted that the fact that information might be exempt from the general rule of public access should not preclude a government institution from disclosing the information when it wishes to do so[50]. Not all documents covered by an exemption will be particularly sensitive, and it would be undesirable to preclude disclosure of exempt documents where the government institution has resolved that there would be no harm in disclosure. This same line of reasoning should apply to the drafting of exemptions with respect to subject access and correction rights. Even though information might be exempt from the general rule of access, it should be permissible for the institution to disclose the information if it deems it appropriate to do so.

The principle of segregability

We recommend that here, as in the freedom of information context, where portions of a document contain exempt material, a reasonable effort should be made to segregate the exempt portion and release the remainder of the record to the individual. In this way, the fullest possible realization of the rights of the data subject will result.

Exemptions of records, not "systems of records"

We do not feel that it would be a sound policy to exempt entire systems of records or, indeed, entire collections of record

systems maintained by particular government institutions. We favour the broadest possible application of fair information practices and principles, and we believe that their implementation is likely to be most broadly secured by ensuring that the data subject has access and correction rights to any system. We appreciate, of course, that there must be exemptions to the general principle of access and that the effect of these exemptions may generally preclude access to a particular system. Where a system contains only highly sensitive information, denial of access will be inevitable. On the other hand, we do not feel that it would be useful to make the entire system as such exempt from the act and thus create a potential haven of secrecy for information which could, without prejudice to governmental interests, be disclosed to the data subject.

What exemptions from the general right of subject access and correction should be adopted? We will consider first those exemptions which form a part of our freedom of information proposals and which are applicable to the subject access context; we will then consider the desirability of a number of additional exemptions which are not included in our freedom of information proposals.

First, the following exemptions set forth in our freedom of information proposals appear to be appropriate in the context of subject access and correction rights:

- . Cabinet documents
- . Information received in confidence from other governments
- . International relations and national defence
- . Law enforcement
- . Confidentiality preserved by other statutes
- . Solicitor-client privilege
- . Information creating unfair advantage or harm to negotiations

With particular reference to the law enforcement exemption, it should be noted that the freedom of information exemption listed as one of the reasons for denying access to law enforcement information would be that it would "constitute an unwarranted invasion of privacy" of the individual to whom the information pertains. Clearly, this would not apply where the data subject is himself requesting access to the file. Nonetheless, the other

features of the law enforcement exemption would apply to the request of the data subject, and would have the general effect of excluding from access investigative and intelligence information contained in law enforcement files.

In addition to the adoption of the freedom of information exemptions referred to above, we recommend the addition of exemptions relating to:

- . information whose disclosure would constitute an unwarranted invasion of another individual's personal privacy;
- . evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for appointment to public or judicial office or for the awarding of government contracts and other benefits, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the enactment of this legislation, under an implied promise that the identity of the source would be held in confidence;
- . medical information the disclosure of which would prejudice the health of the data subject;
- . correctional records whose disclosure could reasonably be expected to (1) seriously disrupt an individual's institutional, parole, or mandatory supervision program; (2) reveal information supplied on a promise of confidentiality, express or implied; or (3) result in physical or other harm to that individual or any other person;
- . research and statistical records.

A brief explanation of the rationale for each of these exemptions should be given.

Unwarranted invasion of the privacy of another person

It is conceivable that a record containing personal information about the data subject may also contain sensitive information about another person. In our view, the information relating to the other person ought to be deleted from the record unless it can be shown, on the basis of the balancing test set forth in our

freedom of information proposals, that, in all the circumstances, the proposed invasion of the other person's privacy is warranted.

Opinion and evaluative material

Several briefs drew our attention to the problem of possible impairment of the government's ability to obtain frank opinions if such evaluations were invariably to be made available to the data subject. While we recognize some legitimacy in this concern, it is our view that, to the extent possible, mechanisms ought to be adopted which will permit the maximum communication of information in a record to the data subject. Thus, we have suggested that the information be made exempt only to the extent that its disclosure would reveal the identity of the informant or referee. Moreover, it is our hope that the Data Protection Authority could assist institutions in designing their review procedures in such a way as to minimize the need to engage in confidential data collection of this kind.

Medical information

Concern about the imposition of a general right of subject access to personal information in medical files has been frequently expressed. Traditionally, patients have not been accorded rights of access to their files[51]. Modern privacy protection statutes, however, have generally made medical information available to the data subject. Various mechanisms have been proposed for dealing with the difficult situation in which the possibility of harm to the patient could result from disclosure of information. Here, of course, the primary concern relates to the disclosure of their files to psychiatric patients. Some schemes propose that where the attending physician believes that the disclosure to the patient may be harmful, disclosure is to be made to an intermediary physician who would, in turn, decide whether to disclose information to the patient[52]. Other schemes propose that the determination as to whether disclosure to a patient will be unduly prejudicial in a particular case ought to be made by an independent tribunal[53]. While there is general agreement about the need for an exemption of this kind, there is some disagreement as to the mechanism for resolving disputes in particular cases. This matter, we understand, has been the subject of considerable study by the Royal Commission of Inquiry into the Confidentiality of Health Records; accordingly, apart from observing that we are of the view that some mechanism should be established for this purpose, we defer to the more detailed and careful consideration of these issues which that commission has undertaken.

Corrections

In Chapter 27, we referred to the need for confidentiality with respect to certain kinds of information contained in corrections records. Access to correctional files by third parties would be precluded under our freedom of information proposals either by the law enforcement exemption or by the personal privacy exemption. We have therefore not included an exemption relating to correctional material in that scheme. In this, our approach is consistent with the U.S. Freedom of Information Act and the federal Canadian and Australian proposals. In the context of a subject access scheme, however, it is our view that specific reference to correctional matters is required. Exemptions pertaining to corrections are included in both the U.S. Privacy Act and the Canadian Human Rights Act, Part IV. The wording of the provision we have recommended is drawn from the Canadian provision.

Research and statistical records

Personal information which has been gathered exclusively for research or statistical purposes is frequently exempt from the general rule of subject access under U.S. privacy protection schemes[54]. Such material would not be available under the Canadian Human Rights Act, Part IV, inasmuch as that statute provides for right of access only to information contained in data banks maintained for administrative purposes. The rationale for depriving the individual of right of access to these materials is simply that the administrative inconvenience involved is too great a price to pay for access to information which is of no potential significance to determinations made about the individual. Although we are in agreement with this view, we wish to make two further recommendations with respect to research and statistical data. First, if the data is disclosed in individually identifiable form, for some purpose other than an additional research or statistical use, we believe that the data should not be exempt[55]. Further, we believe that the exclusion of research and statistical data from the subject access scheme must be coupled with the recognition of a general principle of "functional separation" between research and statistical data on the one hand and administrative data on the other. The significance of this principle is that personal information gathered for research purposes will, as a general rule, not be used in the making of determinations about the data subject. We make recommendations with respect to this general principle and its statutory implementation in section F of this chapter.

FEES

In our freedom of information proposals, we have made recommendations with respect to the question of fees to be chargeable upon the exercise of the right of access. In essence, we recommended that charges relate only to the cost of reproducing the material and that, except under extraordinary circumstances, no charge be levied for the cost of retrieving the document. We also recommended that the statute provide that a governmental institution may waive the fees in appropriate cases and, where the public interest demands it, must waive the fees charged to the individual requester.

We believe that similar considerations apply in the present context, and recommend that a similar set of provisions relating to the charging of fees be established with respect to subject access and correction rights. We would add, however, that in cases where the data subject prevails in the matter of a requested correction, no charges should be made with respect to the exercise of the access and correction right.

TIME LIMITS

In our freedom of information proposals, we made recommendations with respect to the imposition of time limits within which government institutions must respond to requests from the public for access to government documents. Similar provisions should be applicable to subject access requests.

It is our recommendation that a reply to the initial request must be made within thirty calendar days. Again, as we indicated in our earlier discussion, we hope that successful implementation of these access schemes would permit agencies to respond more quickly than this, and that it might ultimately be feasible to shorten the statutory period.

We repeat the recommendation that a further extension of time for replying to the initial request be implemented in accord with the principles set forth in our earlier discussion.

Finally, with respect to a request to correct information in the record, we recommend that such requests be reviewed within a thirty-day period and that a report of the decision be forwarded to the data subject. Again, we recommend that the institution be permitted an additional ten days' grace where good cause can be shown for the delay.

FORM OF DENIAL OF ACCESS AND CORRECTION REQUESTS

When a decision is made by a governmental institution to deny a data subject's request for access to his file, notice of the decision (as set out in our freedom of information proposals) should include the following information:

- . the statutory provision under which access is refused;
- . an explanation of the basis for concluding that the information sought is covered by the exempting provision;
- . the availability of further review and how it can be pursued;
- . the name and title of the person responsible for the decision.

In cases where the government institution decides it will not accede to a requested correction of the record, the agency will, in notifying the data subject of this decision, indicate the nature of the individual's right to file a statement of disagreement and to appeal the decision.

RECOMMENDATIONS

1. Data subject access and correction rights should be conferred with respect to government records containing personal information, the terms "records" and "personal information" being broadly defined in accord with the definitions set forth in the Canadian Human Rights Act, Part IV.
2. Information contained in the records should be provided to the data subject in a form which is comprehensible to him.
3. A data subject should be permitted to authorize another individual to obtain access to records containing personal information on his behalf.
4. Where practicable, the information should be communicated in such a manner as to indicate the general terms and conditions under which the information in question is maintained and used.
5. Data subjects should have an opportunity to challenge the accuracy, relevance, timeliness or completeness of the information contained in personal records concerning them and, in the event of unwillingness on the part of the record keeper

to alter the record, should be permitted to file a statement of disagreement to be stored with the record in question.

6. Record keepers should assume an obligation to communicate corrections, or the existence and nature of statements of disagreement, to future users of the information and, further, should contact prior users of the information or the sources from which the information was obtained in accord with any instructions in this regard imposed by the Data Protection Authority.
7. Provisions exempting certain kinds of information from the general rule of subject access should be designed along the following lines:
 - a. the exemptions should be permissive rather than mandatory in the sense that even though information may be exempted from access, the institution in question would be permitted to disclose the information if it wishes to do so;
 - b. where portions of a record are exempt, a reasonable effort should be made to segregate the exempt portions and release the remainder of the record to the data subject;
 - c. the exemptions should be designed to exempt particular information types rather than entire data banks or systems of records;
 - d. the following exemptions set forth in our freedom of information proposals should be applicable in the context of subject access and correction requests:
 1. Cabinet documents
 2. law enforcement
 3. international relations and national defence
 4. information received in confidence from other governments
 5. confidentiality preserved by other statutes
 6. information creating unfair advantage or harm to negotiations
 7. solicitor-client privilege

- e. in addition to the foregoing, exemptions relating to the following should apply to subject access and correction requests:
 - 1. information the disclosure of which would constitute an unwarranted invasion of another individual's personal privacy;
 - 2. evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for appointment to public or judicial office or for the awarding of government contracts and other benefits, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the enactment of this legislation, an implied promise that the identity of the source would be held in confidence;
 - 3. medical information the disclosure of which would prejudice the health of the data subject;
 - 4. correctional records whose disclosure could reasonably be expected to
 - (i) seriously disrupt an individual's institutional, parole, or mandatory supervision program;
 - (ii) reveal information supplied on a promise of confidentiality, express or implied, or
 - (iii) result in physical or other harm to that individual or any other person.
 - 5. research and statistical records.
- 8. Fees may be charged, unless waived by the record keeper, only for the cost of copying the material in question. No charges should be made with respect to the exercise of the access and correction rights, where the data subject has prevailed in the matter of a requested correction.
- 9. A time limit of thirty calendar days should be imposed for response to the request for access, and an additional thirty days with respect to requests for corrections. Each period could be extended for a further ten-day period where good cause can be shown for delay.

10. When a decision is taken by a government institution to deny a request for access, notice of this decision should be given to the data subject and should include the following information:
 - a. the statute or provision under which access is refused;
 - b. the basis for concluding that the information sought is covered by the exempted provision;
 - c. the availability of further review and how it can be pursued;
 - d. the name and title of the person responsible for this decision.
11. In notifying a data subject of denial of a requested correction of the record, the record keeper should indicate the nature of the individual's right to file a statement of disagreement and the right to appeal the decision.

F. RESEARCH AND STATISTICAL DATA

In previous sections of this report we have considered aspects of the use of government data for research or statistical purposes. Thus, in our recommendations for a freedom of information scheme, we suggested that one of the reasons for granting access to identifiable government data under a freedom of information act would be to permit research and statistical uses of government data by the requesting party[56]. In appropriate cases, an FOI request for access to data could be granted even though the data in question contained identifiable information about named individuals. We also recommended that a transfer of information for research or statistical purposes be one of the permitted exemptions to the general "no transfer" rule[57]. This recommendation was made, however, with the proviso that the Data Protection Authority should have the power to approve the terms and conditions under which such data could be used, in order to ensure the maintenance of proper safeguards to protect the confidentiality of the information.

It should be noted that each of the foregoing proposals would be applicable to identifiable personal data, regardless of the purpose for which it was first gathered. For example, medical information gathered in the course of administering the provincial health benefits scheme could be made available to medical researchers in order to carry out epidemiological research.

We have recommended that data gathered exclusively for research or statistical purposes be exempt from the general rule that data subjects should have access to information concerning them[58]. The argument for such an exemption, we suggested, is that, given the expense involved, the granting of subject access would serve no purpose, inasmuch as the records have no administrative significance as far as the individual is concerned.

We now turn to the question of whether identifiable personal data gathered in the first instance for a research or statistical use should be used for administrative purposes. If it is accepted that, as a general rule, research and statistical records should not be used for such purposes, are there any exceptional circumstances in which such uses should be permitted? Finally, inasmuch as research material gathered for the purposes of one research project might have subsequent value in the context of another, should special provision be made for the granting of access to such materials for subsequent research projects?

With respect to the first point, we have concluded that recognition should be given to a general "principle of functional separation," which would hold that a clear distinction must be drawn between research and statistical material and data gathered for administrative purposes. As a general rule, material gathered exclusively for the former purpose could not be used for the latter without the consent of the data subject. This is not to say that material gathered exclusively for one research or statistical purpose could not subsequently be used for another. Indeed, it may be desirable to encourage such subsequent use in appropriate cases -- although here we favour a requirement of DPA approval -- in order to facilitate economical use of research resources and to avoid burdening research subjects with further contact and inconvenience. Our concern is to prevent subsequent administrative use of the data.

Our desire to ensure the immunity of research material is premised on two considerations. The first relates to "fair information practices." Denial of access for administrative purposes would conform to the expectations of the data subject and would protect him from inadvertent exposure to administrative action as a result of participation in a research project. This point is particularly compelling if, as we have recommended, research and statistical data is to be exempt from the general rule of subject access. The second consideration arises from our previously expressed view that fair information practices laws ought to be designed in such a way as to encourage rather than frustrate the conduct of responsible and potentially valuable research activities. Public confidence in the confidentiality of research exercises is essential to their success. By ensuring that inadvertent administrative harm cannot flow from participation in

government research projects, research subjects will be encouraged to volunteer accurate personal information. In reaching these conclusions, we have been much influenced by the views of the Privacy Protection Study Commission (PPSC)[59] and those expressed by Professor Flaherty in his Commission research paper[60]. Both of these reports have argued for the adoption of a principle of functional separation.

At the same time, we recognize that there are situations in which subsequent access to research and statistical material should be granted, even though this will involve disclosure of identifiable personal data. Here too, we were much influenced by the views of the PPSC[61].

First, an exemption should be permitted where disclosure of the data might be of assistance in dealing with serious threats to the health and safety of an individual. The individual in question might be the data subject himself (for example, where potentially beneficial follow-up from a research project may necessitate communication of data to another agency). It is possible, however, that the individual in question might be a third party who, for example, is being threatened by or has otherwise been placed at risk by the data subject. One possible illustration of this could arise in the context of hostage-taking incidents where psychiatric information concerning the perpetrators might be of assistance in attempting to respond effectively to the emergency. In such circumstances it might be desirable to give law enforcement authorities access even to sensitive psychiatric data.

Second, although we do not favour general access to research and statistical data for law enforcement purposes, there may be situations in which access to identifiable data will be instrumental in permitting an investigation of violations of confidentiality requirements which have been imposed on researchers or government personnel. This use does not derogate from the general principle of functional separation. Indeed, its purpose is to lend the principle even greater support.

Third, we suggest that there is a public interest in ensuring that public monies are properly spent. We favour access to identifiable data when it is necessary in order to permit the proper authorities (such as the Provincial Auditor) to conduct an audit or evaluation of research or statistical activities carried out or financed by the government.

Finally, in order to ensure that potentially valuable research material remains available for further research or statistical purposes, transfer of the data in identifiable form to the Archives of Ontario should be expressly permitted.

Apart from such exceptional circumstances, however, we feel that the general principle of functional separation should be strictly observed.

One final matter must be mentioned. In his Commission paper, Professor Flaherty argued persuasively for the establishment of a provincial statistical bureau similar to those established in British Columbia and Quebec. In essence, such bureaus operate as the provincial equivalents of Statistics Canada. The creation of such a bureau, in Professor Flaherty's view, would facilitate greater access by the government of Ontario to research data gathered by the statistical agencies of other governments[62]. Further, such an agency could perform a useful role in protecting the confidentiality of government research and statistical data and in the promotion of controlled dissemination of data for research and statistical purposes. As Professor Flaherty noted, similar recommendations were made to the government by the Committee on Government Productivity in its 1973 report. Our view is that the formulation of recommendations on this subject would carry us beyond our mandate to inquire into freedom of information and privacy protection problems. We nevertheless feel that Professor Flaherty's views are worthy of consideration, and we therefore recommend that an examination of the need for the establishment of a statistical bureau be undertaken by the government.

RECOMMENDATIONS

1. Controls should be placed on the subsequent use of individually identifiable data which has been collected or prepared by a government department or agency solely for research or statistical purposes.
2. These controls should be premised on the recognition of a general principle of "functional separation": data gathered for research or statistical use should not subsequently be used for administrative purposes without the consent of the data subject, except in the following circumstances:
 - a. where disclosure will assist in dealing with a serious threat to the health and safety of an individual;
 - b. where access is necessary in order to carry out an investigation of confidentiality requirements placed on researchers or government personnel;
 - c. where access is necessary in order to permit the proper authorities to conduct an audit or an evaluation of research or statistical activities carried out or financed by the government;

- d. where identifiable data are transferred to the Archives of Ontario because of their historical value.
3. We commend Professor Flaherty's proposals for the establishment of a provincial statistical bureau to the government of Ontario as worthy of further consideration.

G. THE DUTY TO RECORD DISCLOSURE

A number of U.S. privacy statutes require that an agency holding identifiable personal information about an individual must keep track of its disclosures to other agencies or individuals (whether inside or outside the government) and must give an accounting of these disclosures to the data subject either upon request or upon the exercise of an individual's right to have access to his file.

The HEW report identified this concept as an essential feature of its privacy protection scheme. The report argues that the privacy interest of individuals will be protected only if they are afforded the right "to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it"[63]. More specifically, the report recommends that each agency should:

maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given.... This requirement will contribute significantly to an organization's capacity to detect improper dissemination of personal data[64].

There does not appear to be much direct evidence on Canadian public attitudes toward the desirability of an accounting of disclosures requirement. The federal study, in its survey of industry attitudes toward the privacy implications of computer use, yielded equivocal evidence on this point[65]. It is doubtful, however, that this survey is of much assistance here. The survey respondents were record keepers rather than individual citizens and it is not surprising that those who are engaged in maintaining personal data systems might have mixed feelings about the imposition of a duty to keep track of all disclosures.

Our view is that the imposition of a requirement for an accounting of disclosures is justified on the basis that the knowledge that such a record is maintained and that access can be had to it will result in greater citizen confidence in the fairness of government record-keeping practices. A sense of privacy invasion

results from lack of knowledge of the uses given to files containing personal information; this will be lessened by the existence of an accounting requirement. For this reason, we favour such a requirement and recommend that access to the record of disclosures be given to data subjects. The accounting should be given both as a matter of course to an individual who seeks access to his file and in response to a specific request for an accounting.

An accounting requirement will also facilitate communication of corrections of records. We have recommended that as a corollary to the individual's right to correct or amend personal records, it is desirable to impose a duty on the record holder to convey these corrections to other agencies to which it has previously communicated incorrect information. Maintaining an accounting of previous disclosures is obviously essential to compliance with this duty.

Finally, an accounting requirement is justified by the need to facilitate the monitoring of agency compliance either through internal audit procedures or by the Data Protection Authority. Our recommended privacy protection scheme imposes duties to refrain from certain kinds of disclosures. The agency may itself wish to maintain internal control procedures which would include keeping track of disclosures to third parties. In any event, the enforcement of these duties through the activities of the DPA -- described in Chapter 34 of this report -- would be much more easily sustained if the agency were obliged to keep such records.

It follows from the second and third of these justifications that an accounting must be kept of all disclosures or transfers of data. We appreciate, however, that if individual data subjects were to be made aware of all law enforcement disclosures, effective law enforcement could be frustrated for the reasons identified in our discussion of the general problem of access to law enforcement material. Accordingly, we recommend that although an accounting of law enforcement disclosures be maintained, such disclosures need not be revealed to the data subject.

The arguments against imposing an accounting principle of this kind rest primarily on questions of cost and administrative convenience. Although we weigh such considerations with great care, we think it possible to exaggerate the practical difficulties involved in compliance with this proposal. Computer systems can be programmed so as to include "logging" devices and indeed, many systems are so designed simply to keep track of users for billing purposes. As far as manual systems are concerned, it should be possible to devise systems for recording bulk transfers or to simply annotate individual files as use is made of them. Nonetheless, the administrative burdens of this proposal are far from inconsequential; it may therefore be helpful to consider

briefly the recent U.S. experience in operating a scheme of this kind and compare to it the much less burdensome scheme adopted in the Canadian Human Rights Act, Part IV.

U.S. PRIVACY ACT OF 1974

Section 3(c)(1) of the Privacy Act provides that each agency shall keep an accurate accounting of the date, nature and purpose of each disclosure of the record to any person or agency, and the name and address of the person or agency to whom the disclosure is made. There are two express exceptions to this rule. First, a record is not required to be kept of disclosures to officers and employees of the same agency which maintains the record if those officers and employees have a "need to know" the information in the individual's record. Second, no record is required to be kept of disclosures made under the Freedom of Information Act. As a more general matter, however, the disclosure of information upon a written request by the subject or with his prior consent appears to be outside the provisions, and accordingly no accounting need be kept of disclosures of this kind.

The agency is obliged to disclose its accounting of previous disclosures to the data subject under section 3(b)(3) with one exception: the agency is not required to disclose its accounting of disclosures which it has made to another agency for civil or criminal law enforcement purposes.

In sum, then, the individual data subject is entitled to an accounting of all disclosures of information by the agency which were not:

1. requested by or consented to by him;
2. within the agency on a need-to-know basis;
3. under the FOIA;
4. for a law enforcement purpose.

It should be noted that many types of disclosures remain subject to an accounting requirement. As noted previously, agencies are permitted to disclose personal records pursuant to a provision which allows disclosure for a "routine use" (defined as a use for a purpose "compatible with the purpose for which it was collected") without the consent of the data subject[66]. Although there thus appears to be a broad area of agency disclosures for which consent is not necessary, at least an accounting of such disclosures must be kept and (except for cases covered by the

exemptions enumerated above) that accounting must be accessible to the data subject.

The PPSC Report indicates that the federal agencies have found the obligation to keep an accounting of disclosures very burdensome. It is alleged to represent "26 per cent of the operating costs of the Act and requires extra effort by agency employees on an almost daily basis." Moreover, it is reported that few individuals have asked for an accounting of disclosures made of their records (although the report suggests that this may very well be attributable to the fact that citizens generally may not be aware of their right to do so)[67].

Notwithstanding these concerns, the PPSC concluded that this requirement should be maintained. Indeed, the PPSC criticized the disclosure requirements as not being sufficiently stringent since, as has been noted above, internal disclosures on a need-to-know basis are excluded from the accounting. The PPSC felt that internal uses of the data should also be subject to an accounting[68].

In their submissions to the PPSC, some federal agencies suggested that subjecting routine uses (such as inter-agency disclosures for payroll purposes) to accounting imposed an excessive burden. The PPSC did not consider the requirement to be unduly onerous. The PPSC suggested that requiring agencies to render only an "accounting" (as opposed to a "record") of disclosure permits them to maintain general records relating to frequent bulk transfers of data. They can reconstruct a list of past disclosures if a data subject makes an inquiry[69]. The PPSC did recommend, however, that the accounting rules in the Privacy Act be amended. It was the commission's view that the essential reason for requiring an accounting was to permit the propagation of corrections. Accordingly, the PPSC recommended in its proposed redraft of the Privacy Act that the agency be required to maintain an accounting of disclosures:

1. to all prior recipients of the record to whom the agency could be reasonably expected to propagate a correction pursuant to the (new and more onerous) propagation requirement, and
2. any other recipients of which the agency could be reasonably expected to be aware.

The PPSC's revised provision requires more complete accounting than that of the Privacy Act of 1974, in that it contains no exemption for internal agency uses nor does it explicitly exempt disclosures based on prior request or consent of the subject. This may appear to impose an unnecessary burden, but it is, we feel, both a desirable and a manageable obligation. The

possibility of fraudulent requests suggests the desirability of maintaining such records. Moreover, the data subject may wish to know that a disclosure to a third party (to which he has given his consent) has actually occurred. Where a disclosure is made to a third party upon the specific request of the subject, the request form itself could be easily inserted in the data subject's file and annotated when the requested disclosure is made. It should be noted that such subject consents are likely to be blanket in form and may often be given by a data subject who is unaware of the full implications of such a consent. Accordingly, an accounting of such disclosures would be consistent with the general principles of data protection which the Privacy Act seeks to preserve.

CANADIAN HUMAN RIGHTS ACT, PART IV

Although the Canadian act states that every individual is entitled to "ascertain the uses to which [personal] records have been put since the coming into force of this Part," it does not impose a duty on agencies to maintain a log of disclosures to other agencies or third parties[70]. Presumably, the act supports this purported entitlement through a combination of two methods. First, the individual is entitled to be consulted and must consent to any "non-derivative" use of the information for an administrative purpose[71]. (It is true that section 52(3) deems consent to be given in a case where notice in writing has been furnished and the individual has not replied, but it is reasonable to assume that in most cases notice of "non-derivative" use will be effectively made.)

Second, with respect to "derivative uses," the act provides that the minister (in whose discretion, it will be recalled, a use of personal data may be deemed to be "derivative," or consistent with the use for which it was compiled) must publish annually a listing of the derivative uses of records which come under his control[72]. The data subject can thus familiarize himself with such uses, although there may be some delay in his ability to learn of new derivative uses until they appear in a minister's annual statement.

This scheme has the obvious merit of eliminating the burden of record keeping associated with an accounting requirement. In our view, however, there are two serious deficiencies in these provisions as a device for implementing fair information practices principles. First, the lack of an accounting requirement means that neither the agency nor the data subject has much prospect of conveying corrections to other recipients of the individual's personal information. Second, for the broad category of "derivative" uses, the individual is not consulted; accordingly, he will have no effective knowledge of a substantial body of data disclosures

in which his personal information is used by the federal government.

RECOMMENDATIONS

1. In order to facilitate subject awareness of uses made of personal data, propagation of corrections to other users of the data, and monitoring of compliance with the rules controlling data transfers, it is recommended that:
 - a. record keepers be required to maintain an accounting of all disclosures or transfers of identifiable personal data;
 - b. the record subject have access to the accounting of disclosures, apart from disclosures for law enforcement purposes.

H. RECOMMENDATIONS

A PUBLIC RECORD OF GOVERNMENT PERSONAL DATA BANKS

1. We recommend that governmental institutions be required to publish an annual systems notice with respect to each personal record-keeping system they maintain and to publish new systems notices when new systems are established or substantial modifications to existing systems are effected.
2. Annual systems notices and new systems notices should be required by statute to contain the following information:
 - a. the name and location of the data bank;
 - b. the legal authorization for its establishment;
 - c. the types of information or data items maintained in the system;
 - d. the principal uses of the information and the categories of users to whom disclosures from the system are typically made;
 - e. the categories of individuals for whom records are maintained in the system;
 - f. the policies and practices applicable to the system with respect to storage, retrievability, access controls,

retention and disposal of information maintained in the system;

- g. the title, business address, and business telephone number of the official responsible for the operation of the system.
- 3. Governmental institutions should not be required to include items of information in systems notices which would otherwise be exempt from public access under the proposed freedom of information legislation.
 - 4. An annual compendium of systems notices should be published by the government of Ontario. The index could be modelled on the Index of Federal Information Banks, published by the Treasury Board of Cabinet of the government of Canada pursuant to the provisions of the Canadian Human Rights Act, Part IV.

COLLECTION OF PERSONAL INFORMATION

Our recommendations with respect to the control of data collection practices are as follows:

- 5. The Data Protection Authority should have the responsibility to comment, where it deems it appropriate to do so, on the privacy protection implications of proposed legislative schemes or government programs.
- 6. A statutory duty should be imposed on government departments and agencies to collect only such personal information as is either expressly authorized by statute or necessary to the proper administration of a lawfully authorized administrative activity.
- 7. The Data Protection Authority should have the power to:
 - a. make binding determinations as to whether a particular data collection meets the standards suggested in paragraph 6;
 - b. require a government department or agency to cease a collection practice which violates paragraph 6 and destroy collections of data gathered in violation of this standard.
- 8. A government department or agency which is engaged in the collection of personal information should inform the

individual from whom the information is requested, in writing, of the following:

- a. the legal authority for the collection of the information;
 - b. the principal purpose or purposes for which the information is intended to be used;
 - c. whether disclosure is mandatory or voluntary and the consequences of failure to provide the information;
 - d. such proposed use and dissemination of the information as can be reasonably anticipated;
 - e. the types of additional information and the sources to be used to verify the information;
 - f. the name, title and business telephone number of a public official who can answer any questions the individual may have with respect to the data collection;
 - g. whether the individual or some other person will have access and correction rights with respect to the information.
9. The Data Protection Authority should have the power to determine the extent and manner in which information required in paragraph 8 shall be communicated to the individual from whom the information is requested. It may, in appropriate circumstances, excuse the government department or agency from engaging in communication of this kind.
10. To the extent practicable, a government department or agency should collect information directly from the data subject when an adverse determination may result.
11. The Data Protection Authority should have the power to excuse a government department or agency from compliance with paragraph 10.

STANDARDS FOR MAINTAINING THE INTEGRITY AND SECURITY OF DATA

12. Record keepers should maintain all records used in making a determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual concerned.

13. The Data Protection Authority should be empowered to make final determinations of the application of the standards set forth in paragraph 12 to specific data-gathering systems.
14. The gathering of intelligence information for law enforcement purposes should constitute the exception to the general standards set out in paragraph 12; provided, however, that the information is stored in such a way as to signal its unreliability to users.
15. The duty should be imposed to destroy personal data no longer useful for the accomplishment of the objectives for which it was originally collected, unless destruction would potentially deprive the data subject of some benefit resulting from its storage or unless the data is to be stored, on terms or conditions approved by the DPA, for use as a research resource or for ultimate transfer to the Archives of Ontario as data of historical value.
16. Record keepers should establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats to their security or integrity.
17. The DPA should make final determinations of the applications of the standards set forth in paragraph 16 to specific data systems.

CONTROLLING TRANSFERS OF DATA

18. No disclosure or transfer of identifiable personal data should be made unless the disclosure comes within one of the following exceptional cases:
 - a. disclosure under the freedom of information provisions;
 - b. a "routine" use as defined by the PPSC, i.e., a use for a purpose which is:
 - i. compatible with the purpose for which the information in the record was collected or obtained, and
 - ii. consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected or obtained, and
 - iii. where disclosure is made to an officer or employee of the agency who has need for the record in the

performance of his duties, access may be granted where it is necessary and proper for the performance of the agency's own mission and functions;

- c. disclosure for a "collateral use" as defined by the PPSC, i.e., disclosure pursuant to statutory provisions, provided that such provisions establish specific criteria for the use or disclosure of such information;
- d. disclosure by a law enforcement agency to another law enforcement agency in Canada or to a law enforcement agency in a foreign country, provided that in the latter case the disclosure is made pursuant to a written agreement, a treaty or a legislative authority;
- e. disclosure to a person pursuant to his showing of compelling circumstances affecting the health and safety of an individual;
- f. in compassionate circumstances, disclosure to facilitate contact with the next of kin, or a friend, of an individual who is injured, ill or deceased;
- g. disclosure to a member of the Legislative Assembly who has been authorized by a constituent to make an inquiry on his behalf or, where the constituent is incapacitated, has been authorized by a relative or legal representative of the constituent;
- h. to the Provincial Auditor;
- i. to the Ombudsman of Ontario;
- j. to the Data Protection Authority;
- k. to the Director of Fair Information Practices;
- l. to the Fair Information Practices Tribunal;
- m. to the federal government in order to facilitate the auditing of shared-cost programs;
- n. to the Archives of Ontario;
- o. to Statistics Canada.

SUBJECT ACCESS AND CORRECTION RIGHTS

19. Data subject access and correction rights should be conferred with respect to government records containing personal information, the terms "records" and "personal information" being broadly defined in accord with the definitions set forth in the Canadian Human Rights Act, Part IV.
20. Information contained in the records should be provided to the data subject in a form which is comprehensible to him.
21. A data subject should be permitted to authorize another individual to obtain access to records containing personal information on his behalf.
22. Where practicable, the information should be communicated in such a manner as to indicate the general terms and conditions under which the information in question is maintained and used.
23. Data subjects should have an opportunity to challenge the accuracy, relevance, timeliness or completeness of the information contained in personal records concerning them and, in the event of unwillingness on the part of the record keeper to alter the record, should be permitted to file a statement of disagreement to be stored with the record in question.
24. Record keepers should assume an obligation to communicate corrections, or the existence and nature of statements of disagreement, to future users of the information and, further, should contact prior users of the information or the sources from which the information was obtained in accord with any instructions in this regard imposed by the Data Protection Authority.
25. Provisions exempting certain kinds of information from the general rule of subject access should be designed along the following lines:
 - a. the exemptions should be permissive rather than mandatory in the sense that even though information may be exempt from access, the institution in question would be permitted to disclose the information if it wished to do so;
 - b. where portions of a record are exempt, a reasonable effort should be made to segregate the exempt portions and release the remainder of the record to the data subject;

- c. the exemptions should be designed to exempt particular information types rather than entire data banks or systems of records;
- d. the following exemptions set forth in our freedom of information proposals should be applicable in the context of subject access and correction requests:
 - 1. Cabinet documents
 - 2. law enforcement
 - 3. international relations and national defence
 - 4. information received in confidence from other governments
 - 5. confidentiality preserved by other statutes
 - 6. information creating unfair advantage or harm to negotiations
 - 7. solicitor-client privilege
- e. in addition to the foregoing, exemptions relating to the following should apply to subject access and correction requests:
 - 1. information whose disclosure would constitute an unwarranted invasion of another individual's personal privacy;
 - 2. evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for appointment to public or judicial office or for the awarding of government contracts and other benefits, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the enactment of this legislation, an implied promise that the identity of the source would be held in confidence;
 - 3. medical information whose disclosure would prejudice the health of the data subject;
 - 4. correctional records whose disclosure could reasonably be expected to:

- i. seriously disrupt an individual's institutional, parole, or mandatory supervision program;
 - ii. reveal information supplied on a promise of confidentiality, express or implied; or
 - iii. result in physical or other harm to that individual or any other person;
 - 5. research and statistical records.
26. Fees may be charged, unless waived by the record keeper, only for the cost of copying the material in question. No charges should be made with respect to the exercise of the access and correction rights, where the data subject has prevailed in the matter of a requested correction.
27. A time limit of thirty calendar days should be imposed for response to the request for access, and an additional thirty days with respect to requests for corrections. Each period could be extended for a further ten-day period where good cause can be shown for delay.
28. When a decision is taken by a governmental institution to deny a request for access, notice of this decision should be given to the data subject and should include the following information:
- a. the statute or provision under which access is refused;
 - b. the basis for concluding that the information sought is covered by the exempted provision;
 - c. the availability of further review and how it can be pursued;
 - d. the name and office of the person responsible for the decision.
29. In notifying a data subject of denial of a requested correction of the record, the record keeper should indicate the nature of the individual's right to file a statement of disagreement and the right to appeal the decision.

RESEARCH AND STATISTICAL DATA

30. Controls should be placed on the subsequent use of individually identifiable data which has been collected or prepared

by a government department or agency solely for research or statistical purposes.

31. These controls should be premised on the recognition of a general principle of "functional separation": data gathered for research or statistical use should not subsequently be used for administrative purposes without the consent of the data subject, except in the following circumstances:
 - a. where disclosure will assist in dealing with a serious threat to the health and safety of an individual;
 - b. where access is necessary in order to carry out an investigation of confidentiality requirements placed on researchers or government personnel;
 - c. where access is necessary in order to permit the proper authorities to conduct an audit or an evaluation of research or statistical activities carried out or financed by the government;
 - d. where identifiable data are transferred to the Archives of Ontario because of their historical value.
32. We commend Professor Flaherty's proposals for the establishment of a provincial statistical bureau to the government of Ontario as worthy of further consideration.

THE DUTY TO RECORD DISCLOSURES

33. In order to facilitate subject awareness of uses made of personal data, propagation of corrections to other users of the data, and monitoring of compliance with the rules controlling data transfers, it is recommended that:
 - a. record keepers be required to maintain an accounting of all disclosures or transfers of identifiable personal data;
 - b. the record subject have access to the accounting of disclosures, apart from disclosures for law enforcement purposes.

CHAPTER 33 NOTES

- 1 S.C. 1976-77, c. 33.
- 2 5 U.S.C. s. 552a, passed as part of Pub. L. 93-479.
- 3 Treasury Board, Administrative Policy Manual, Chapters 410, 415, 420, and 425, all dated December 1978.
- 4 Personal Privacy in an Information Society (Washington: USGPO 1977) cited hereafter as PPSC Report.
- 5 Great Britain, Report of the Committee on Data Protection (1978; Cmd. 7341) cited hereafter as Lindop Report.
- 6 See Chapter 34, Section C of this report.
- 7 Canadian Human Rights Act, Part IV, s. 51(2).
- 8 Somewhat more extensive reporting requirements are imposed in the U.S. Privacy Act. More elaborate requirements have been recommended by the PPSC: PPSC Report, Appendix 4, The Privacy Act of 1974: An Assessment, 81-92, 166-67.
- 9 See NSW Privacy Committee Report 1975-78 (Sydney: 1979) 12, para. 5.1.
- 10 S. 552a(e)(1). "Each agency that maintains a system of records shall -- (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."
- 11 This suggestion is based on the Treasury Board guidelines, which suggest that the individual supplying the information should be advised of his own access and correction rights or, in a case where the individual is supplying information about another person, of that other person's access and correction rights. See Administrative Policy Manual, Chapter 410, "Information Banks: Design and Collection," 10-11.
- 12 Ibid.
- 13 Recommendations to the same effect were made by the Privacy Protection Study Commission. See PPSC Report, App. 4, 125-26.
- 14 Administrative Policy Manual, Chapter 410, 13-16.

- 15 Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967) 7.
- 16 See Chapter 27.
- 17 Records, Computers and the Rights of Citizens (Cambridge: Massachusetts Institute of Technology, 1973) cited hereafter as HEW Report.
- 18 See Chapter 29.
- 19 PPSC Report, App. 4, 124-25.
- 20 Ibid., 57-67.
- 21 Commission on Federal Paperwork, Confidentiality and Privacy (Washington: USGPO, 1977) 65-66, cited hereafter as CFP Report.
- 22 PPSC Report, App. 4, 134-35.
- 23 Ibid., 160.
- 24 Chapter 29, Section G.
- 25 PPSC Report, App. 4, 125.
- 26 CFP Report, 68-69.
- 27 Administrative Policy Manual, Chapter 415, 11-14.
- 28 See generally, Report of the Royal Commission of Inquiry into Civil Rights (Toronto: Queen's Printer, 1968) Vol. 1, Chapters 28-34; and J.A. Fontana, The Law of Search Warrants (Toronto: Butterworths, 1974).
- 29 5 U.S.C. 552a, s. b(7).
- 30 PPSC Report, App. 4, 58.
- 31 M. Brown, B. Billingsley and R. Shamai, Privacy and Personal Data Protection (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980), cited hereafter as M. Brown. See also Chapter 27 of this report.
- 32 See Volume 2, Chapter 14, Section J (the privacy exemption to the FOI scheme) and Chapter 33, Section F (third-party access to data gathered for a research of statistical purpose).

- 33 R.S.O. 1970, c. 240 as amended.
- 34 Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972) 154-55, cited hereafter as Privacy and Computers.
- 35 HEW Report, xxvi.
- 36 Administrative Policy Manual, Chapter 420.
- 37 The Consumer Reporting Act, S.O. 1973, c. 97.
- 38 The Education Act, S.O. 1974, c. 109.
- 39 S.C. 1976-77, c. 33, s. 49.
- 40 Ibid.
- 41 PPSC Report, App. 4, 114-15.
- 42 For statutory language embodying such a requirement, see PPSC Report, 155.
- 43 Administrative Policy Manual, Chapter 420, 18-19.
- 44 See Chapter 34 of this report.
- 45 5 U.S.C. 552a, s. (d)(4).
- 46 PPSC Report, App. 4, 71-73, 124, 164-65.
- 47 Ibid., 2-83.
- 48 Exemption (b)(5).
- 49 Bill C-15 (31st Parliament, 28 Elizabeth II, 1979) received first reading on October 24, 1979, but the government was defeated before it proceeded further.
- 50 We further indicated limitations on this general principle with respect to commercially valuable information and personal information relating to third parties: see Volume 2, Chapter 14.
- 51 See generally, T.G. Ison, Information Access and the Workmen's Compensation Board (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 4, 1979) 81-102.

- 52 See, for example, U.S. Privacy Act (f) 3, and see M. Brown, 42-59 and 491-94. See also Administrative Policy Manual, Chapter 420, 17-18.
- 53 See, for example, Quebec, An Act Respecting Health Services and Social Services, S.Q. 1971, c. 48 as amended, s. 7; Alberta, The Alberta Hospitals Act, R.S.A. 1970, c. 174 as amended, s. 35(6), and The Mental Health Act, S.A. 1972, c. 118 as amended, s. 50; Nova Scotia, The Public Hospitals Act, R.S.N.S. 1967, c. 249 as amended, s. 63(4). All four of these statutes provide for judicial review of denials of access.
- 54 See, for example, Privacy Act, 5 U.S.C. 552a (a)(6), (k)(4).
- 55 For the expression of a similar view, see PPSC Report, 603-04.
- 56 See Volume 2, Chapter 14, Section J.
- 57 See Section D of this chapter.
- 58 See Section E of this chapter.
- 59 PPSC Report, Chapter 15.
- 60 D.H. Flaherty, Research and Statistical Uses of Ontario Government Personal Data (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 5, 1979) 80, cited hereafter as Flaherty.
- 61 PPSC Report, 574-83.
- 62 Flaherty, Chapter II.
- 63 HEW Report, 41.
- 64 Ibid., 56. The PPSC, in reviewing the operation of the accountability provisions of the Privacy Act of 1974, indicated that the accounting of disclosures requirement has three objectives: (1) to provide an individual with a listing of uses of disclosures of the record about him; (2) to facilitate the propagation of corrections; and (3) to promote internal agency auditing and compliance with monitoring: see PPSC Report, App. 4, 70.
- 65 Privacy and Computers, 38.
- 66 S. 3(d)(3).

- 67 PPSC Report, App. 4, 103.
- 68 Ibid., 69-71, 103, 122.
- 69 Ibid., 123.
- 70 S.C. 1976-77, c. 33, s. 52(1)(b).
- 71 S. 52(2).
- 72 S. 52(1).

Administration and Enforcement

INTRODUCTION

In light of the serious nature of the informational privacy protection problem we have found to be inherent in the record-keeping practices of modern governments, and in particular of the government of Ontario, we have recommended the establishment of a strong legislative data protection model. In essence, we propose the establishment of a statutory framework which will require government record keepers to abide by fair information practice principles, and which will confer on the citizen rights of access to and correction of personal records concerning him held by the provincial government.

We appreciate that the scheme we have set forth is a complex one; its complexities have been dictated, we believe, by the complexities of the phenomena it seeks to regulate. Similarly, the administration and enforcement mechanisms we propose as appropriate devices for implementing our recommendations are not of simple design.

At the risk of oversimplification, the administrative and enforcement tasks involved in our scheme may be broken down into three categories:

- day-to-day operation of data banks in compliance with the regulatory scheme;
- data regulation, or elaboration of the statutory standards to ensure that particular data banks comply with the scheme, and to facilitate government planning in the establishment of new data banks in accordance with the scheme's requirements;
- dispute resolution with respect to data subject complaints concerning collection of data, the exercise of access and correction rights, and compliance with transfer controls.

In brief, we propose that the institutional responsibilities for the accomplishment of these tasks be assigned in the following manner. First, the day-to-day operations of the government personal information banks must obviously be the responsibility

of the governmental institution on whose behalf the record system is maintained. We recommend further, however, that each such institution appoint an official, termed by us the "responsible keeper," whose responsibility it shall be to ensure that particular data banks are operated in compliance with the regulatory scheme. The data regulation task is to be assumed by a body we have called the Data Protection Authority (DPA). The DPA will establish standards for the collection, maintenance and security of data; these standards will spell out in greater detail the necessarily general standards set out in the statute. The DPA will approve the application of these standards to particular data banks held by the various agencies and ministries of the government. For example, the statute will indicate that "adequate security" must be maintained with respect to sensitive personal data. The DPA will establish security standards which must be adopted by the record keepers and will approve security arrangements of particular data banks. Similarly, while the statute will impose a duty on agencies to collect only that personal data necessary for their purposes, the DPA will approve the specific collection proposed for particular data banks. Apart from these regulatory responsibilities, the DPA will be assigned a research and advisory role with respect to data protection issues arising in the context of government information practices, and with respect to data-gathering activities in the private sector.

Finally, we propose that the dispute resolution role be channelled through the same mechanism as that proposed for disputes arising under our freedom of information proposal: we recommend that aggrieved citizens be encouraged to bring their complaints to the Director of Fair Information Practices who will have the power to investigate, to excuse the data subject from supplying improperly requested data, to order the granting of access to a data subject, to order the correction of information contained in a personal data file, or to require compliance with data transfer rules. As with freedom of information disputes[1], appeals from the Director could be taken to the proposed Fair Information Practices Tribunal and be subject to judicial review on matters of law by the Divisional Court of the Supreme Court of Ontario pursuant to the provisions of The Judicial Review Procedure Act[2].

We now turn to a more detailed description of the various elements of our scheme for administration and enforcement. We will set out what we see as the ideal model for the implementation of our privacy protection proposals, and a proposal for a transitional phase of implementation in which a portion of the data regulation task might be undertaken under the direct supervision of the Management Board of Cabinet.

A. THE ROLE OF THE MINISTRIES AND OTHER GOVERNMENTAL INSTITUTIONS[3]

Clearly, record holders themselves will assume the greatest burden in terms of administering a fair information practices statute on a day-to-day basis. Agencies of the government must:

- review all data systems and information practices;
- train personnel in handling personal records so as to conform to rules under the statute;
- satisfy the notice requirements, including those relating to transfers;
- redesign information collection instruments and reform information collection methods;
- place controls over information transfers;
- keep records in an accurate, relevant, timely and complete manner, deleting or destroying data no longer required;
- ensure the security and confidentiality of records;
- implement subject access and correction procedures;
- apply exemptions on a case-by-case basis.

B. THE "RESPONSIBLE KEEPER"

To ensure that there is an administrative focal point for the implementation of our scheme, we recommend that a particular individual be given authority to administer the statute at the agency level. This person would assume responsibility for implementing the regulatory scheme and would provide a point of contact for inquiries both from the public and from the regulatory authorities. Although it might be feasible for some agency heads to assume this authority in certain circumstances, in general they have neither the specialized expertise nor the time to address numerous records management and informational privacy matters. Moreover, record subjects would have great practical difficulty consulting agency heads about informational privacy problems. Accordingly, most jurisdictions with fair information practices or data protection legislation have implemented the Swedish concept of the "registrar-accountable" or "responsible keeper." Under the Swedish Data Bank Statute (1973), every "register of persons" or

collection of personal records must be overseen by a designated "registrar-accountable," who interprets and implements statutory rules, assembles applications for data bank operation, takes responsibility for record maintenance and confidentiality, processes subject access and correction requests, and performs other duties described in the statute. The "responsible keeper" approach has also been endorsed by the U.S. Privacy Protection Study Commission, which found

that those agencies that have established formal, structured approaches and mechanisms to implement the Privacy Act are the most successful in their implementation of the Act. They have provided the best training for their personnel, have issued detailed, consistent internal guidelines, and have devised procedures for auditing their own compliance with the Act[4].

In sum, the responsible keeper concept appears to be a useful tool, worthy of consideration in any legislated data protection scheme, for introducing the notion of accountability at a level lower than the agency itself, for overseeing compliance with the statute by agency personnel and for assisting record subjects in the exercise of their rights, particularly their subject access rights.

C. THE DATA PROTECTION AUTHORITY

As we have indicated above, we believe it would be desirable to establish a regulatory authority whose broad mandate will be that of assuring compliance with our proposed legislative scheme. Its powers and duties should be defined by regulations, and it should report to the Premier. The kinds of duties appropriate for such an authority include setting consistent inter-agency standards, educating both the public and government employees about privacy legislation, publishing an index of information banks, inspecting and approving the establishment of data banks and their information practices, evaluating agency performance under the act, reviewing legislation, and engaging in research about broad policy issues. The body or bodies designated to perform these functions may also be required to make annual reports to the legislature.

While we appreciate that there may be some resistance to the suggestion that a new regulatory authority of this kind be established, we have come to the conclusion that this is a desirable initiative for a number of reasons. First, we believe that it would be a false economy to permit each agency to attempt to implement the statutory standards for its own record-keeping

practices. We think it would be unfortunate, for example, if agencies attempting to comply with the statutory standard relating to the security of data systems put in place more extensive and expensive security arrangements than necessary to meet the legislative standard. (Some U.S. experience suggests that unnecessary extravagance in this particular area is a realistic possibility.) Further, we think it would be most unfortunate if governmental agencies were to be confronted with subsequent determinations that data banks which had been established at great expense were not being operated in compliance with the law. A system of granting credible and binding approvals in advance of the establishment of such systems seems to be sound privacy protection planning as well as sound economics. Finally, the statutory scheme we propose must necessarily be somewhat general and imprecise in its language. It would be useful to have an authoritative source of detailed interpretations of the statutory language for specific applications.

One of the most difficult questions with which we have wrestled in fashioning our privacy protection proposals is that of an appropriate institutional location for a data protection authority. The Commission first considered the use of an existing administrative body, the advantages of which are primarily ones of cost. If the Management Board Secretariat were charged with supervision and administration of privacy legislation in Ontario, for example, it would merely extend its present jurisdiction over governmental data banks and record management, erasing the need for the establishment of a new body. It might also be argued that the Management Board would be better suited for this role than would an independent body because it already has an ongoing relationship with agencies and therefore would not encounter the resistance which might be met by a new organization. Moreover, the Management Board has statutory powers to regulate government administrative practices and can therefore ensure compliance with its directives[5].

However, the Commission found the arguments against the use of an existing administrative structure compelling. In previous chapters, we have argued that the current state of affairs, in which privacy protection is one of a cluster of concerns for government information systems planners, is inadequate. It is to be expected, for example, that those charged with the responsibility of administering a government program would be inclined to develop information systems which are both extremely efficient and geared to permit extensive data collection concerning the individuals whom the program is designed to serve. Building in adequate privacy protection safeguards may create inefficiencies which the administrators of a particular program would be disinclined to undertake on their own initiative. The establishment of an independent authority as a source of authoritative guidance on proper

privacy protection practices would ensure that proper safeguards are established. Moreover, the establishment of a separate authority with this mandate would enhance public confidence in the measures taken to protect the privacy of individual citizens, even in cases where the authority's recommendations are no different in substance from measures that would have been adopted by the government administrators on their own initiative.

We have recommended that the DPA, as part of its research and advisory mandate, undertake an examination of privacy protection issues in the context of personal data collection and dissemination in the private sector. Management Board (or a similar government body) would be an inappropriate vehicle for the examination of private sector record-keeping practices. A separate privacy authority would be a more suitable body to investigate and make recommendations about these privacy protection concerns. Thus, recognizing that the strength and credibility of the proposed law will depend on the rigour with which it is administered, overseen and enforced, the Commission recommends that an independent body, appointed by the Lieutenant Governor in Council, and reporting directly to the Premier rather than to the Cabinet, be assigned these responsibilities. To ensure public accountability of the activities of the DPA, reports made to the Premier would be required to be tabled in the Legislative Assembly or otherwise made available to the public.

The experience of other jurisdictions, particularly the United States, also convinced us that adding a data protection mandate to an existing administrative mechanism would be an inappropriate means for implementing a legislated privacy protection scheme. The U.S. Privacy Act empowers the Office of Management and Budget (OMB), assisted by four other federal executive agencies, to develop guidelines and regulations and assist agencies in fulfilling their statutory responsibilities. The Privacy Protection Study Commission (PPSC), a temporary body set up to evaluate the act, claimed that

neither the OMB nor any of the other agencies with guidance responsibilities have subsequently [since the Act's inception] played an aggressive role in making sure that the agencies are equipped to comply with the Act and are, in fact, doing so,...[that] early momentum appears to have been lost,...[and] that there seems to be more variation in agency practice than is necessary, and certainly more than is desirable if a prime object of the Act is to make it easy for individuals to have a say in how agencies collect, use and disseminate records about them[6].

In the U.S. case, the absence of vigorous supervision of the implementation of the act has apparently resulted in inconsistent and sometimes contradictory agency rules, administration, training and compliance, a very small number of complaints brought by individuals, little follow-up on citizen complaints and underutilization of civil and criminal sanctions. In contrast, evidence from European countries (particularly Sweden) employing independent agencies to perform the administrative enforcement and reporting functions required by privacy legislation indicates that such bodies have succeeded in achieving institutional change, in handling citizen complaints, and in promoting public confidence in the effectiveness of the data protection law. The available evidence indicates that there are advantages in establishing an independent Data Protection Authority. Creation of such a body is consistent with the recommendations of a previous Ontario study[7]. The Data Protection Authority would perform many of the same functions as the U.S. Privacy Protection Study Commission[8], the proposed U.S. Federal Privacy Board[9] and a number of state-level information practices bodies[10]. Specifically, the DPA would have powers to:

- . oversee the notice and indexing provisions;
- . monitor, review and evaluate agency rules and performance concerning any matter relating to the act;
- . approve the establishment of new data banks;
- . render interpretations of the application of the statutory data management duties to specific data banks;
- . provide consultative assistance relating to information practices;
- . review legislation to assess its implications for privacy, and make recommendations about such legislation to government;
- . engage in research concerning privacy protection issues;
- . receive complaints from ordinary citizens about general information practices;
- . report annually on its activities to the Premier and to the legislature.

Unless a supervisory body, such as the DPA, can exercise powers to investigate and make judgments about information practices, it may be weak and ineffective. Thus, we believe that it would be useful to permit the DPA to give binding interpretations

of the application of various data management standards to specific data banks. A data bank which complied with a DPA interpretation of the security arrangements required for a specific data bank would be deemed to have met the statutory standard. A data bank containing information whose collection has been approved by the DPA would be deemed to have complied with the duty to collect only that personal data necessary for the purposes of a particular program. The making of authoritative determinations of this kind would occur as a matter of course in granting approvals for the establishment of new data banks. With respect to existing data banks, the powers of the DPA could be invoked at the request of a particular institution or on the initiative of the DPA itself.

D. DISPUTE RESOLUTION: ACCESS AND CORRECTION RIGHTS

With respect to the disposition of citizens' complaints concerning the exercise of their statutory rights of access and correction, it is our view that the dispute resolution mechanism we recommended under our freedom of information act proposals could usefully be employed in this context as well, for a number of reasons. First, the nature of the dispute between the individual and the government agency relating to subject access is similar to a freedom of information dispute: the data subject seeks access to his file, and the government agency protests that the information in question is exempt from access under one of the statutory rules. As we noted earlier, some of the exemptions relating to freedom of information requests will be identical to exemptions to the subject access rule. This confirms our view that it would be desirable to have one dispute settlement mechanism offering authoritative interpretations of these provisions. Second, we think it would be confusing to individual citizens to be required to follow two different appeal processes with freedom of information and subject access requests. An individual engaged in a dispute with a particular agency may, for example, wish to have access to his own personal file and to what we have elsewhere termed "internal law" relating to the subject matter of the dispute. We believe that it would be sensible to resolve both of these matters through the same appeal process. Finally, as we have pointed out several times in this report, the central notion of a freedom of information scheme -- the granting of a right of public access to government documents -- creates a tension between the public's right to know and the individual citizen's right to privacy. We believe that a more sensitive reconciliation of these competing interests will be encouraged if the appeal mechanism responsible for determining where the balance lies in a particular case also assumes responsibility for the determination of appeals relating to the data subject access and correction rights.

We propose that aggrieved individuals be encouraged to bring their complaints to the Director of Fair Information Practices. The director would be empowered to investigate the matter in any way he sees fit and require the agency in question either to disclose information to the data subject or enter a statement of correcting information in the data subject's file. For similar reasons, data subjects' specific complaints that a particular request for information or a proposed transfer of information is improper should be handled by the Director of Fair Information Practices. The director should be empowered to excuse the data subject from supplying the requested information where the collection exceeds that which is permitted by law. Further, the director should have the capacity to forbid proposed transfers where they contravene the standards relating to data dissemination.

Appeals from decisions of the Director of Fair Information Practices could be taken to the Fair Information Practices Tribunal on a matter of fact or of law. A further right to judicial review on matters of law would be available under The Judicial Review Procedure Act to the Divisional Court of the Supreme Court of Ontario.

E. THE INTERIM AND TRANSITIONAL PHASE: AN ALTERNATIVE PROPOSAL

We are aware that the establishment of a Data Protection Authority with the powers described above may give rise to some misgivings, particularly in the initial phase of implementation when it may be thought that an overly aggressive and swift implementation of fair information practices principles might result in substantial dislocation of a considerable number of government data-gathering operations.

Further, it may be thought that inasmuch as the Management Board Secretariat is currently in possession of substantial expertise with respect to the operation of data systems, it would be unwise to attempt to build from scratch a DPA which would undertake the rather considerable responsibilities we have ascribed to it.

We presume that it was for reasons of this kind that the federal government adopted, in the Canadian Human Rights Act privacy protection scheme, the device of assigning data regulation responsibilities to the Treasury Board. The government of Ontario, for similar reasons, may feel that it is both expedient and wise to assign data regulation responsibilities to the Management Board Secretariat for the initial phase of implementation of a privacy

protection scheme. The arguments favouring such an approach are weighty and we are not unsympathetic to the adoption of a mechanism of this kind. Our view, however, is that such a proposal should be adopted only for an interim and relatively short period of time. For the reasons set out in this chapter, we remain convinced that ultimately an independent authority should be established.

If an interim plan of this kind were to be adopted, it would be critical, we believe, to ensure that rights of inspection and comment with respect to data regulation activities be conferred on the Director of Fair Information Practices. If there is to be a period of trial and error, we would recommend that the director be given a mandate to contribute to the discussions leading to the formulation of policy by the Management Board Secretariat. Presumably, the commencement of the research and advisory role of the DPA with respect to private sector data protection problems would be either postponed until the authority is established as a separate functioning body or assigned, in the interim, to the Director of Fair Information Practices.

In an earlier chapter of this report, we suggested that the issues raised by government's collection and use of personal data concerning citizens raises fundamental questions concerning the relationship between the citizen and the government. We remain of the view that in any institutional framework established for the purpose of defining this relationship, an independent voice must be created whose mandate it will be to articulate and seek due recognition of the citizen's right to privacy.

F. RECOMMENDATIONS

In summary, we make the following recommendations with respect to the administration and enforcement of the data protection scheme:

1. To ensure that an administrative focal point is established in each institution subject to the scheme, we recommend the appointment of a "responsible keeper" within each institution whose responsibility would be to ensure that data banks subject to his supervision are operated in compliance with the requirements of the data protection law.
2. A Data Protection Authority should be established, which would have a broad mandate to supervise the implementation of the data protection scheme and to engage in research on privacy protection implications of the record-keeping practices of public and private institutions.

3. The Data Protection Authority should be a body established for the specific purpose of implementing the data protection scheme. It should be appointed by the Lieutenant Governor in Council and should report directly to the Premier. The powers and duties of the DPA should be defined by regulations passed by the Lieutenant Governor in Council, and an annual report of its activities should be made to the Premier, who would be obliged to table it in the Legislature or otherwise make it available to the public.
4. For an interim transitional period, it may be appropriate to assign the responsibilities of the DPA to the Management Board of Cabinet.
5. The resolution of disputes between data subjects and governmental institutions maintaining personal data should be handled by the dispute resolution mechanisms established for the purposes of resolving similar disputes under the freedom of information law. Aggrieved individuals should be entitled to seek the intervention of the Director of Fair Information Practices and, on appeal, the Fair Information Practices Tribunal.
6. Apart from his responsibilities with respect to dispute resolution, the director would be empowered to comment more generally on the privacy protection implications of information practices which have become subject to his scrutiny.
7. As in the context of our freedom of information proposals, the Director of Fair Information Practices and the Fair Information Practices Tribunal would be empowered to obtain access to exempt documents and to examine them in camera in the absence of the parties. Proceedings before the director would be informal in nature. Proceedings before the tribunal would be subject to the provisions of The Statutory Powers Procedure Act. The tribunal would be empowered to entertain representations from governmental institutions in the absence of the applicant where this is necessary to facilitate a full explanation of the reasons for non-disclosure of a particular document.

CHAPTER 34 NOTES

- 1 See Volume 2, Chapter 15 of this report.
- 2 S.O. 1971, c. 48.
- 3 In Chapter 32 of this report, we have made recommendations as to the range of governmental institutions which should be subjected to the proposed statutory scheme.
- 4 Privacy Protection Study Commission, The Privacy Act of 1974: An Assessment (Appendix 4 of Final Report) (Washington: USGPO, 1977) 97.
- 5 Management Board of Cabinet Act, S.O. 1971, c. 12, ss. 3, 6.
- 6 The Privacy Act of 1974: An Assessment, 18-21.
- 7 Ontario Privacy Project Task Group, Report and Recommendations (Toronto: Management Board of Cabinet, 1976).
- 8 See Chapter 29, Section E of this report.
- 9 One of the precursors of the U.S. Privacy Act of 1974 was Bill S.148, introduced in the Senate by Senator Ervin. The bill proposed that a Federal Privacy Board be established in the executive branch. The board would consist of five members (none of whom would be present civil servants) appointed by the President with the advice and consent of the Senate. The board's administrative and oversight functions were to include (1) receiving and reviewing annual systems notices from agencies, and proposals for new or modified systems; (2) publishing an annual index of data systems; (3) consulting with the heads of agencies; (4) making rules to assure compliance with the act; and (5) reporting annually on its activities to Congress and the President. In terms of enforcement, the board was to be granted broad powers to (1) inspect any records, systems or record-keeping practices, compelling the production of necessary documents by subpoena; (2) upon the determination of a violation of the act or regulation, after a hearing, issue a cease and desist order; (3) recommend to the Attorney General that an action be brought against an offending agency or individual in the appropriate U.S. District Court; (4) conduct open, public hearings on all petitions for exceptions or exemptions from provisions. Under the proposed act, the board was also directed to give assistance to and resolve disputes between

individuals and agencies at the request of individuals. The bill is reproduced in U.S. Senate and U.S. House of Representatives, "1976 Source Book on Privacy," Legislative History of the Privacy Act of 1974 (Washington: USGPO, 1976) 6, 9-12, 17, 22.

- 10 See Chapter 29, Section F of this report.

Civil and Criminal Liability

In previous chapters, we have set out our scheme for the statutory implementation of fair information practices policies. Under our scheme, certain statutory standards are to be imposed on government record keepers. Certain rights to obtain access to personal files and seek their correction are to be afforded to the subjects of personal information files. We have further recommended that mechanisms ensuring adequate administration and enforcement of the scheme be established. In this chapter, we consider what civil and criminal liabilities should be imposed when the provisions of the scheme have not been followed. More specifically, should the individual who has personally suffered harm as the result of an unfair practice be entitled to seek monetary compensation for such injuries in a civil action for damages? We then consider the need for the establishment of new statutory offences in order to encourage compliance with the scheme.

A. CIVIL LIABILITY: THE REMEDY OF MONETARY DAMAGES

A list of hypothetical cases in which a civil remedy of monetary damages might be appropriate may help to clarify the issue:

1. Welfare authorities fail to keep accurate information or unreasonably refuse to make a requested correction, with the result that the individual is unfairly denied welfare benefits.
2. An agency improperly discloses information relating to psychiatric treatment of an individual with resulting humiliation, embarrassment, and injury to his reputation.
3. An agency improperly discloses information relating to psychiatric treatment, with the result that the data subject loses his job or is denied an employment opportunity.
4. An agency refuses access to a file. The data subject would have been able to successfully petition for a benefit of some kind if he had been able to obtain the

file to rebut the incorrect information contained therein.

5. An individual submitting an application to participate in a government program of some kind is asked to supply sensitive personal information -- for example, relating to an unusual and potentially embarrassing medical condition -- which is not relevant to the operation of the program in question. The individual suffers considerable distress as a result of being required to disclose such information to the government.

In each of these illustrations, privacy rights granted to the individual under the privacy protection scheme have been infringed, with resulting injury to the data subject. The injuries vary in nature and extent. Actual pecuniary loss occurs in illustrations 1, 3 and 4, whereas the injuries in the other cases constitute "psychological" injury of some kind. The issue to be addressed here, then, is whether claims for money damages should be allowed in compensation for some or all injuries of these kinds.

One preliminary point should be considered. Our earlier discussion of privacy law[1] indicates that there is no realistic prospect that causes of action for money damages for "privacy invasion" would be made available under existing common-law principles. Although it may be that when statutory duties associated with privacy protection are imposed by law on government record keepers a civil cause of action for money damages could arise from a tort law analysis premised on the existence of a breach of statutory duty, we understand this to be a somewhat tenuous source of redress[2]. Rather than rely on the somewhat difficult principles of law associated with a tort analysis, we believe it to be preferable to specifically provide for any damages remedy in the statute itself.

Turning to the merits of this issue, it is our view that a strong argument can be made in favour of the availability of a civil damages remedy. While the availability of such a remedy may encourage proper conduct, our primary concern is simply one of wishing to ensure that wrongfully-caused injuries are not left without remedy. The illustrations set forth above suggest that genuine economic loss can result from breaches of privacy duties. We believe that where measurable economic harm has resulted from wrongful conduct, a remedy should lie.

More than this, we are of the view that breaches of fair information practices which result in what we have termed "psychological" injuries also constitute a wrongful invasion of

the individual's privacy interest which should be subject to an award of damages (albeit a sum which may be difficult to calculate in particular cases). Instances such as illustrations 2 or 5 above may be deeply troubling to the individual involved. Such injuries, we feel, should be compensable under the provisions of the privacy protection scheme. Although the measurement of loss poses obvious difficulties, we understand that similarly difficult problems of measuring loss are satisfactorily resolved by the courts in various areas of the law of torts[3] and more recently, in the law of contracts[4]. The difficulties inherent in measuring this form of loss should not, in our view, preclude attempts at doing so.

Having resolved that a civil damages remedy should be made available under our scheme, a number of ancillary questions arise. Should compensation be allowed only where the conduct of the public official is in some sense malevolent or willful? We are opposed to such a restriction on liability for two reasons. First, it will not be much consolation to the aggrieved data subject to be advised that the public official did not realize that he was acting in flagrant violation of the privacy legislation. Second, it may be very difficult for a data subject to prove that the public servant was possessed of such a state of mind. Hence the government should be liable, regardless of the intentions or bona fides of the public servants. We feel, however, that personal liability should only be imposed on a public servant if he acts in willful disregard of his statutory duty. As we indicated in previous chapters, we have some sympathy for the problems of the public servant attempting in good faith to comply with the provisions of what must inevitably be a rather complex legislative scheme[5].

We have given consideration to, and rejected, the possibility of awarding punitive or exemplary damages in cases of this kind. The theory underlying punitive damages is that mere compensation is not a sufficient penalty to impose on the government if liability is to act as a disincentive to committing such breaches. For example, provisions enabling the award of punitive damages have been enacted by Parliament in order to discourage illegal electronic surveillance or wiretapping[6]. It is our view, however, that legislation of this kind is more appropriate in the context of wiretapping infractions which per se constitute a major invasion of one's privacy. Until it is demonstrated that there are compliance problems in Ontario, we would hesitate to recommend such a measure.

A further alternative would be to propose a fixed amount of minimum damages. It may be argued that such a measure would lead to ease of quantification and, further, provide a strong

disincentive for disregard of the act by public officials. We fear, however, that the granting of a substantial minimum claim for privacy defaults might induce people to bring actions with respect to matters of little or no consequence to them. We are reluctant to encumber our proposals with a device of such dubious merit.

Finally, it must be determined whether the civil liability which we propose is to attach to all breaches of all duties imposed by the statute, or if it should apply only to a subset of breaches of particular importance to data subjects. Our general view on this point is that where identifiable harm to the individual results from a failure to comply with the statute, the remedy should be available. It may be possible, however, to identify some duties, breaches of which are not at all likely to result in genuine injury, and exclude them from the compensation scheme. This approach has the obvious virtue of precluding frivolous lawsuits with respect to breaches of the duties in question. It seems unnecessary, for example, that a claim for damages would result from the publication of an inaccurate systems notice or from failure to comply with highly technical security standards. It would, however, be essential to ensure that the damages remedy is available where identifiable harm has resulted from breaches of the following duties:

- . the duty to collect only authorized or relevant data;
- . the duty to refrain from disclosure or transfer of data;
- . the duty to give access to files and make corrections;
- . the duty to propagate corrections.

B. THE ESTABLISHMENT OF PROVINCIAL OR "QUASI-CRIMINAL" OFFENCES

One of the more difficult questions to be faced in designing privacy protection schemes is to determine whether the sanction of provincial "quasi-criminal" offences should be employed so as to encourage compliance with the statute. As we have indicated earlier, we are disinclined, as a general matter, to recommend the establishment of new provincial offences. Yet, we believe that there are strong arguments for the adoption of a strictly limited set of offence provisions in the proposed privacy legislation.

As a preliminary point, it is useful to note that such sanctions have often been used by the government of Ontario to protect privacy. As we have noted earlier, legislation currently in force which preserves the confidentiality of government-held

personal data commonly imposes sanctions on public servants who fail to comply with the confidentiality rules. For example, The Health Insurance Act[7] provides, subject to certain exemptions, that information concerning OHIP subscribers must not be disclosed by government employees. Any breach of this provision constitutes an offence under the act and renders the public servant in question liable to a fine of not more than \$2,000. A Commission research paper[8] reveals that the majority of statutes containing confidentiality provisions also stipulate that it is an offence to breach the confidentiality rule. The imposition of penalties on individuals engaging in transfers of personal data prohibited under our recommended privacy protection scheme would thus not involve a substantial departure from the existing Ontario practice in such matters.

Improper disclosure, however, is not the only manner in which duties imposed under our scheme could be breached. What must be considered is whether all of the duties imposed under the scheme should be enforced by sanctions of this kind, or whether it is sufficient to impose sanctions for breach of some subset of the more important duties. The U.S. Privacy Act has adopted the latter approach, and offers, we believe, a model worthy of emulation.

Section 552a(i) of the U.S. act stipulates three different offences in the following terms:

(i)

- (1) CRIMINAL PENALTIES. -- Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an

agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

The first offence occurs if an individual makes a disclosure of individually identifiable records which is prohibited by the statute. The offence is committed only if the accused individual knew that the disclosure was prohibited and nonetheless "willfully" disclosed the information. The second offence relates to the "no secret data banks" principle. Anyone who "willfully" maintains a system of records without complying with the statutory requirements concerning the publication of information about data banks is guilty of an offence. The third offence relates to the obtaining of personal information about others under false pretenses. An offence of this kind would occur if someone were to falsely identify himself as the data subject in order to obtain access to a file under the subject access rules.

Of particular interest, in our view, is that each of these provisions requires a "guilty mind" in the accused. The individual in question must, in other words, have intended to commit the prohibited act. We note also that the first type of offence relating to improper disclosure requires further that the officer or employee of an agency have known that the disclosure was prohibited by law. This would enable an employee to raise a defence by saying either that he was unaware of the prohibition or that he reasonably believed that the prohibition did not extend to the material in question. This requirement obviously responds to a concern that agency personnel who unwittingly breach the act should not be subject to the criminal sanction, even where they were unaware of the laws governing the situation.

In our view, these provisions offer a balanced solution to the sanctions issue. The prohibitions relating to the conduct of public servants are narrowly confined to what appear to be the two types of misconduct which most offend the spirit of the legislation. Clearly, a strong argument can be made for offence provisions relating to improper disclosure. As we have indicated, such provisions already exist in various Ontario statutes. Further, the evidence before the Royal Commission of Inquiry into the Confidentiality of Health Records (the Krever Commission) suggests that, notwithstanding these provisions, improper disclosures of health data may have occurred in Ontario. This suggests that where there is a market for personal information, temptations to improperly furnish such information will be present. It therefore appears necessary to impose sanctions on those who improperly disclose personal data regulated by the privacy protection scheme.

A further reason for isolating improper disclosure for special attention is that once such a disclosure has occurred, the damage, in a sense, cannot be undone. Where other data subject rights, such as access and correction rights, have been infringed, the person who is denied access can appeal such a ruling and ultimately obtain access. There may therefore be less need to invoke offence provisions to discourage improper conduct.

With respect to the "secret data banks" offence, we believe that publicity concerning the nature and existence of government data banks is a basic principle from which much else in our scheme flows. The maintenance of secret information systems so flagrantly and fundamentally violates the object of our proposals that we feel that such conduct must be forcefully condemned by the legislative provisions. Moreover, breaches of this principle may be very difficult to detect; accordingly, a strong incentive for compliance should be embodied in the statute.

The third offence -- obtaining information by false pretenses -- also appears to be a necessary element in the sanctioning scheme. The evidence before the Krever Commission suggests that fraudulent practices of this kind may be commonly employed, particularly by private investigative firms, to obtain identifiable personal data from Ontario government departments and agencies. Again, there are obviously economic incentives for engaging in conduct of this kind and it appears necessary to provide a countervailing incentive through the imposition of a criminal sanction.

Finally, we agree with the approach taken in the U.S. provisions with respect to the mental element included in the definition of each offence. The privacy protection scheme may prove to be a difficult and complex scheme for citizens and public servants to interpret. Accordingly, a generous defence to the improper disclosure prohibition in cases of bona fide error seems appropriate. In cases where a stricter rule of liability should be developed, individual provisions may remain or be placed in discrete statutes. Thus, if it is felt that there is a particular problem with improper disclosure of confidential health data, and that the confidentiality rules are matters about which Ministry of Health employees cannot have much reasonable doubt, a strict liability offence might be imposed. We presume that questions of this kind will be reviewed by the Krever Commission. In our view, however, to impose so-called "strict liability" offences as a general matter is unduly draconian in the absence of evidence of widespread abuse of provisions of this kind.

C. RECOMMENDATIONS

1. We recommend that a civil remedy be made available under the privacy protection scheme in the following terms:

A data subject is to be entitled to monetary damages for identifiable harm resulting from breaches of the following statutory duties:

- the duty to collect only authorized or relevant data;
 - the duty to refrain from disclosure or transfer of data;
 - the duty to give access to files and make corrections;
 - the duty to propagate corrections.
2. The government should be liable for such damages regardless of whether the harmful conduct was intentional, but a public servant should not be subject to personal liability unless he acts in willful disregard of his statutory duty.
 3. The privacy protection legislation should embody provisions creating the following offences:
 - a. improper disclosure of identifiable personal data by a public servant who, knowing that disclosure is prohibited, willfully does so;
 - b. willful maintenance of a data bank in contravention of the requirement of publication of information about data banks;
 - c. obtaining or attempting to obtain personal data under false pretenses.

CHAPTER 35 NOTES

- 1 See Chapter 30 of this report.
- 2 See generally, A.M. Linden, Canadian Negligence Law (Toronto: Butterworths, 1972) hereafter cited as Linden.
- 3 Linden.
- 4 G.H. Fridman, The Law of Contract in Canada (Toronto: Carswell, 1976); S.M. Waddams, The Law of Contracts (Toronto: Canada Law Book, 1977).
- 5 It is not uncommon for the government of Ontario to wholly exempt public servants from personal liability for tortious acts. See generally, Royal Commission Inquiry into Civil Rights, Report No. 3 (Toronto: Queen's Printer, 1971) 2199-2216. We express no opinion as to whether total immunity is appropriate here.
- 6 S.C. 1973-74, c. 50, s. 2: "...a court that convicts an accused of an offence under [the illegal wiretap section] may, upon the application of a person aggrieved, at the time sentence is imposed, order the accused to pay that person an amount not exceeding \$5,000 as punitive damages." See generally, David Watt, The Law of Electronic Surveillance in Canada (Toronto: Carswell, 1978).
- 7 S.O. 1972, c. 91, s. 44.
- 8 T.G. Brown, Government Secrecy, Individual Privacy and the Public's Right to Know: An Overview of the Ontario Law (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 11, 1979) 191-93.

Regulating Use of The Social Insurance Number

As we indicated in Chapter 28, in recent years governmental and non-governmental organizations increasingly have come to use the federal Social Insurance Number (SIN) as a standard identifying number in record-keeping systems containing personal information. In particular, we noted that the use of the SIN was becoming more common in the record-keeping systems of the various institutions of the Ontario provincial government. In this chapter, consideration is given to the possibility of regulating the manner in which the provincial government employs the SIN for these purposes.

The growing use of the SIN in record-keeping systems has led to the development of two different kinds of privacy-related concerns. First, there appears to be considerable public resistance to the use of identifying numbers, and in particular to the use of one single identification number, on the theory that it represents a dehumanizing influence in modern social life. Second, there are concerns that the use of such numbers may result in privacy-invasive record-keeping practices as a result of enhanced capacity to link data bases into what could ultimately amount to a national data bank of personal dossiers on all residents of Canada. The prospects of greater integration of data bases raises, in turn, a number of the informational privacy issues discussed in previous chapters of this report. The possibility that information gathered for one purpose might be used for quite a different purpose is enhanced. The use of data linkage may increase the likelihood that decisions will be based on erroneous information, or on the basis of an individual's historical record rather than his current circumstances or more recent pattern of conduct. In short, it is feared that the use of such dossiers may constitute a form of data surveillance which might operate against the legitimate interests of the individual.

While we do not minimize the gravity of these concerns, the consideration of prohibiting or otherwise regulating the use of identifiers such as the SIN must, in our view, be approached with a number of further considerations in mind. To the extent that objection to the use of the SIN stems from a general resistance to the use of numbers as means of identification of individuals, it must be noted that restriction of the use of the SIN is not likely to result in an overall reduction in the use of identifying numbers. The use of such numbers responds not only to the desire

of public and private organizations to run their record-keeping systems as efficiently as possible, but also to a desire of data subjects that personal record-keeping systems be operated with a high degree of accuracy. If, as consumers, we insist on accuracy in the posting of items to our accounts, and if, as individuals interested in our personal privacy we insist on verification of the identity of persons seeking access to our files, we cannot, at the same time, insist on the elimination of identification systems established with these objectives in view. To some degree, then, the policy choices arising with respect to the use of identification numbers turn on the number of such devices to be used by public and private organizations, and not on whether they are to be used at all.

Of particular concern is whether it is appropriate to permit unregulated growth of SIN use so that this one numbering system comes to dominate public and private sector personal record keeping. This issue was foreshadowed in the federal Canadian task force report on computers and privacy in 1972:

It is possible that a de facto personal identification number will develop in Canada, either through an ever-widening use of the Social Insurance Number (despite its limitations) or indirectly through credit card and bank account numbers. However, it is important to ensure that a single identifying number should not be adopted in Canada, directly or indirectly, without a full explanation and public debate of its merits and consequences[1].

The use of the SIN by both public and private institutions in Canada today is so widespread that it appears to be developing into a de facto single identifying number.

To the extent that increasing SIN use relates to concerns about data linkage, three points must be considered. In the first place, although it is true that under present conditions the use of the SIN facilitates the integration of data bases, such integration is by no means impossible even where the data bases are not based on similar or identical identifiers. The technological capacity to integrate data bases has become very sophisticated, and it appears that in the near future control of the use of standard identifying numbers will have little or no impact on the capacity of record-keeping systems to effect an integration. Thus, it would be unwise to focus on regulation of the use of the SIN as a solution to the data linkage problem. Second, it must be noted that data linkages are not invariably contrary to the best interests of data subjects. Cost efficiencies in record-keeping practices through data linkage may enure to the benefit of data subjects. Data linkage may be essential to the conduct of

valuable research, especially in the medical field[2]. Finally, even those data linkages that may effect a disadvantage to particular individuals may not be viewed by society in general as an unwelcome form of social control. For example, the use of the SIN with respect to income reporting is designed as an aid to enforcement of the obligation of individuals to pay income tax. This is not likely to be widely regarded as an unconscionable use of data surveillance techniques, provided that the fair information practices outlined in this report are employed in the collection and use of this information. In summary, then, the critical question appears to be not whether data linkage should be completely prohibited, but in what circumstances and on what terms and conditions it should be allowed.

The use of identification numbers for record-keeping purposes and their implications for data linkage have, of course, been the subject of concern in other jurisdictions. Experience in the United States with the use of the Social Security Number (SSN) closely parallels the growth of SIN use in Canada. Congressional concern with the unregulated growth of SSN use by government agencies led to the enactment of provisions imposing a moratorium on SSN use by federal, state and local government agencies[3].

In essence, the U.S. provision permits agencies to continue only those SSN uses that are authorized by law. With respect to uses not so authorized, it is unlawful for an agency to deny a benefit to an individual who refuses to supply his SSN. Agencies are required to inform individuals whether the disclosure of SSNs is mandatory or voluntary (and, if it is mandatory, to inform them of the statutory authorization for its collection) and of the uses that will be made of the number by the agency. In 1976, however, more extensive use of the SSN was authorized by provisions contained in the federal Tax Reform Act[4]. That act authorized federal, state and local government agencies to require SSNs for identification purposes from any person affected by any laws relating to tax, general public assistance, driver's licences or motor vehicles. Although SSN use is thus regulated by federal legislation, it is evident that a broad range of uses for these numbers is authorized by statute.

The Privacy Protection Study Commission (PPSC) examined the question of SSN use in its review of the implementation of the Privacy Act of 1974. It was the commission's view that the provisions of the 1974 act restricting the use of the SSN should be retained inasmuch as the provisions "may be somewhat successful in alleviating citizens' concerns about the 'dossier building' capacity of government"[5]. With respect to the underlying concern relating to data linkage, however, the PPSC noted that because of the technological capacity to effect data linkage

without the use of matching numerical identifiers, control of the SSN was an inappropriate means of regulating data transfers. The commission concluded that no useful purpose would be served by imposing restrictions on the use of the SSN other than those contained in the provisions of the Privacy Act of 1974. The commission explained the basis for its conclusions in the following terms:

It is true that if organizations other than the Social Security Administration were forbidden to collect and use the SSN, their exchange of records might be inhibited for a time. Such a prohibition or restriction would, however, be extraordinarily costly and cumbersome, and it would also inhibit record exchanges everyone perceives as wholly desirable along with those perceived to be threatening. Furthermore, organizations which now rely on the SSN would devise alternative methods of identification and authentication that are equally effective for record exchanges.

In any case, the question of the appropriate limitations on exchange of records would remain even if the SSN were done away with altogether. The Commission finds that restrictions on the collection and use of the SSN to inhibit exchange beyond those already contained in law would be costly and cumbersome in the short run, ineffectual in the long run, and would also distract public attention from the need to formulate general policies on record exchanges[6].

Similar views have been expressed in Sweden in a study of the use of identification numbers. Sweden (one of a number of Western European countries maintaining a total population register) has employed a personal identification number in administering its population registration scheme. In its 1978 report, the Swedish Committee on Data Legislation (DALK) did not recommend a prohibition or other restriction on the use of identity numbers in personal data banks. It was more important, in the committee's view, that "attention should be paid to how data are made available and to whom." The committee concluded that

...the elimination of identity numbers in personal registers would place no decisive obstacle in the way of linking of registers....Methods for such purposes exist and are already in use....The elimination of identity numbers would, however, have extensive consequences without attaining the desired result. DALK would particularly emphasize in this context the high costs, which cannot be definitely established without thorough investigations but, to some extent at least, must affect the individuals in the form of higher charges and prices[7].

The use of universal identification numbers, particularly in connection with national registers, has met increasing resistance in European countries in recent years. Accordingly, a number of jurisdictions have imposed controls on the use of such numbers or have withdrawn schemes for the adoption of numbering systems of this kind. Both Norway and France have empowered data protection authorities to regulate the use of personal identification numbers. Under the French statute, permission of a legislative body (the Conseil d'Etat) as well as the National Committee on Data Processing and Freedom must be obtained in order to use the national index (similar to the Canadian federal SIN index) for any type of personal data processing[8]. In its revised Data Protection Act, Germany has abandoned altogether the introduction of a planned standard universal identifier[9]. In Britain, the Lindop Committee on Data Protection recommended that the government assign to an independent data protection authority the responsibility of restricting, in codes of practice having the force of law, the collection and use of any personal identifier intended for any private or public sector personal information system[10]. The committee recommended that a universal personal identifier not be permitted to become a reality merely through ever-expanding use of a convenient existing identifier such as the British National Insurance Number. The committee further recommended that, if the adoption of a universal personal identifier were to be contemplated by the British government, an independent body should be established to consider its privacy implications and the need to enact special legislation prior to the implementation of such a scheme.

Our view is that unregulated growth of the use of the SIN is, under present circumstances, an undesirable development. Although we share the opinion of other committees who have examined this question that the underlying problem of data linkage cannot be resolved through control of the use of the SIN, we are persuaded that the inadvertent adoption of the SIN as a national identification number by incremental growth in its use by both public and private institutions would not be consistent with the public interest in the protection of individual privacy. It is our view that the use of the SIN should be restricted to those situations where the public benefit to be derived therefrom is demonstrably substantial. We think that the SIN should be used for identification purposes by provincial government institutions only where its use has been authorized by law, or (when a comprehensive data protection scheme of the kind we have recommended is implemented) approved by the Data Protection Authority.

We can envisage, in effect, a two-step process by which use of the SIN could be brought under control. First, provisions of the kind embodied in the U.S. Privacy Act of 1974 relating to SSN

use could be adopted, together with statutory authorization for such existing uses of the SIN as are considered by the government to be in the public interest. Once a Data Protection Authority has been established for the purpose of implementing a more comprehensive data protection scheme, however, the ability of the DPA to carefully monitor and regulate data exchanges between data banks would make it an appropriate means of monitoring use of the SIN.

We suggest that legislation could be enacted embodying the following provisions:

- a. No provincial governmental institution shall deny to any individual any right, benefit or privilege provided by law because of that individual's refusal to disclose his Social Insurance Number, unless the institution is authorized to require disclosure of the number (1) by federal or provincial law, or (2) by the Data Protection Authority.
- b. Any provincial governmental institution which requests that an individual disclose his Social Insurance Number shall inform that individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

However, we do not recommend any legislative action until the study of the federal Privacy Commissioner (which we referred to in Chapter 28) with respect to the use of the SIN and its implications for individual privacy becomes available.

CHAPTER 36 NOTES

- 1 Canada, Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972) 89.
- 2 Illustrations of the usefulness of such research are found in D. Flaherty, Research and Statistical Uses of Ontario Government Personal Data (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 5, 1978).
- 3 Privacy Act, U.S. Public Law 93-579 (1974) s. 7.
- 4 U.S. Public Law 94-455 (1976), s. 1211. See, generally, S. Mayer, "Privacy and the Social Security Number: Section 1211 of the Tax Reform Act of 1976" 6 Journal of Computers and Law (1978), 221.
- 5 Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington: USGPO, 1977) 615.
- 6 Ibid., 614.
- 7 Delbetankande av datalagstiftningskommitten (DALK), Personregister -- Datarer Integritet, Summary (Stockholm: DALK, 1978) 344-45.
- 8 Law No. 78-17, Concerning Data Processing, Files and Liberties (1978) Article 18, as translated in U.S. Department of Commerce, Office of Telecommunications, Selected Foreign National Data Protection Laws and Bills (Washington: USGPO, 1978) 43-44.
- 9 "The Personal Number Stymied in Germany?" Transnational Data Reports I, 2 (May 1978) 18.
- 10 Lindop Committee, Report of the Committee on Data Protection (1978; Cmnd. 7341) 261-62.

Mailing Lists

Many individuals find the receipt of substantial quantities of unsolicited mail annoying and privacy-intrusive. In part, the privacy concerns arising with respect to unsolicited mail relate to the fact that one's name and address have been made available from some unknown source to the party forwarding the unsolicited material. In some instances, the unknown source may be a governmental institution which maintains a public register of some kind or has made available a mailing list consisting of the names and addresses of individuals with whom the institution has, for some administrative purpose, been in contact. For those who share the view that unsolicited mail constitutes a threat to privacy values, the sale of mailing lists by government for commercial or other direct mail solicitation purposes may appear to be an objectionable misuse of government-held personal data. In this chapter, we make recommendations with respect to the use of government records for mailing list purposes.

Various legislative experiments attempting to control unsolicited mail and the use of mailing lists have been undertaken in the United States. Before turning to a consideration of recent experience in Ontario, we shall briefly outline these American developments.

Concern relating to unsolicited mail became a political issue in the United States in the 1960s. During this period, members of the public began to voice complaints about the nature and amount of unsolicited advertising and other material they received in the mails[1]. In particular, the receipt of unsolicited sexually-oriented advertising was the subject of a strong public protest. In response, in 1970 Congress enacted a statute which allowed individuals who did not wish to receive this type of mail to fill out a form registering their objections with the U.S. Post Office[2]. The act required firms engaged in this type of mailing to remove the names of these individuals from their lists.

The role of governmental institutions in supplying information from their records to commercial firms for the purposes of compiling mailing lists also became the subject of public discussion during this period. In many cases, direct mail advertising firms were using public records, such as motor vehicle and driver's licence files, occupational licence records, weapons registration forms and tax records as information sources. In

addition, some government agencies compiled lists of names and addresses from their files expressly for the purpose of selling them to commercial firms.

In testimony before the U.S. Privacy Protection Study Commission (PPSC) in 1975, representatives of the two largest U.S. companies engaged in the business of compiling lists for the purposes of direct mail advertising described the extent of the information about individuals which could be gleaned from public records[3]. From official state records, they were able to obtain a list of all car, truck and motorcycle owners and a monthly list of new car owners. The information contained in these records included the owner's name and address, the year, model, make, series, body style and number of cylinders of the vehicles, vehicle identification number (used in safety recall programs) and licence plate number. From this information the companies could infer the owner's sex, type of dwelling (house or apartment), the number of cars owned, and their cost and current market value. The number and kinds of cars owned by an individual may serve as a rough index of his income, and when this is combined with other information from telephone directories, city directories and statistical information from census surveys, mailing list compilers are able to produce detailed information on households. This makes their lists attractive to a wide variety of direct mailers.

The PPSC describes the rules affecting the mailing list practice of government agencies as "one of the murkier areas of public law"[4]. While some records and lists clearly must be made public, the availability of others is less certain. For example, the U.S. Privacy Act of 1974 prohibits a federal agency from renting or selling an individual's name and address "unless such action is specifically authorized by law"[5]. In effect, this provision prohibits federal agencies from marketing lists of names and addresses compiled from government records. On the other hand, it does not override other statutes requiring that various federal agency records (some of which include names and addresses) be made available to the public for inspection and copying. In addition, the Freedom of Information Act may require disclosure of records containing names and addresses in certain cases[6].

At the state level, the use of motor vehicle and drivers' licence registers has been the subject of particular interest. Fourteen states now restrict the use of motor vehicle information for commercial purposes, either through legal regulation or under terms inserted in contracts with list compilers. Some states stipulate that the list compiler can use the information for statistical purposes but not for commercial mailing[7].

In devising its recommendations with respect to mailing lists, the PPSC considered various alternatives for dealing with the problem of commercial use of information contained in public registers or records. Although the commission felt that it would be desirable to permit individuals who did not wish to receive unsolicited advertising to so indicate, the commission emphasized the importance of not undermining the purpose of public records by denying access to information contained in them to the public. The commission rejected as too costly the idea of requiring government agencies to send notices to persons listed on public registers when mailing lists were to be compiled. The commission did recommend, however, that government agencies devise procedures whereby an individual could inform the agency that he did not want his name and address made available for mailing lists, and that this fact be noted in such a way in the public record that a list compiler would become aware of it[8]. Inasmuch as mailing list compilers would not wish to expend their resources in gathering the names of individuals who had signalled such concerns, these techniques would, in the commission's view, result in a self-regulating method of reducing the intrusiveness of mailing list practices.

The commission made further recommendations with respect to the sale by private sector organizations of mailing lists of their customers, members or donors. They expressed the view that the intrusiveness of these practices could be reduced by requiring such organizations to indicate to individuals the possibility that their names and addresses might be used in this way and afford them an opportunity to indicate a preference that their names not be included in such lists.

Against this background, then, we turn to a consideration of recent experiences in Ontario. As far as we have been able to determine, the Ontario government does not engage in any large-scale renting or selling of names and addresses from its files. A study was prepared for Management Board in 1975 of the security and privacy of personal data contained in government records. Nine ministries were surveyed; of a total of 107 files, 8 were used for mailing purposes[9]. The study does not indicate the nature of these files, nor whether the information contained therein is normally available to the public. We understand, however, that commercial sale of mailing lists is not occurring to any significant extent at present.

Although the Ministry of Transportation and Communications has in the past sold information from the vehicle registration files at reduced rates to a commercial firm for mailing list purposes, this practice was discontinued in 1974 in response to expressions of public concern about the use of government information for commercial purposes[10]. It is of interest to note,

however, that the ministry had devised a programming procedure in the early 1970s to remove the names of consumers complaining about junk mail from vehicle lists sold to mailing list compilers. At present, the ministry sells lists in bulk of new vehicle registrations to a commercial firm, but the information may only be resold to automobile manufacturers for the purposes of safety recall programs. The ministry also sells address lists (with owners' names deleted) to automobile parts manufacturers and retailers. The terms of the agreement under which this information is sold stipulate that the buyer will not use the information for sales promotion or other purposes beyond that for which it is sold. Apart from this activity of the Ministry of Transportation and Communications, we are unaware of other instances of the commercial sale of mailing lists based on government-held personal records in Ontario.

In fashioning recommendations with respect to mailing lists, two separate questions must be asked. First, should any attempt be made to permit individuals whose names and addresses are contained in a public register to signal their objection to receipt of unsolicited mail? Second, should governmental institutions be permitted to sell or supply names and addresses (which would not otherwise be made available to the public) under appropriate terms and conditions?

With respect to the first question, it is our view that it would be desirable to encourage governmental institutions to facilitate the expression of such concerns by individuals whose names and addresses are in a public record. On the other hand, we do not feel that it would be practical to impose a requirement that all public registers and other public records be revised so as to accommodate this concern. We recommend, rather, that attention be drawn to this question and that governmental institutions which maintain public records commonly used by mailing list compilers attempt to build into their information systems, to the extent practicable, an opportunity for individuals to signal their desire not to be included in such lists.

With respect to names and addresses contained in government records which would not otherwise be available to the public, we believe that a specific legislative provision would be appropriate. We do not, however, feel it is necessary to adopt a provision similar to that of the U.S. Privacy Act of 1974 prohibiting the sale of mailing lists by governmental institutions. The privacy protection issue presented by the sale of mailing lists would be adequately addressed, we believe, by providing that individuals could be included in such lists only if their consent to use their names and addresses had been secured by the institution in question. It is possible, for example, that individuals applying for a certain type of licence or permit might be quite

willing to have themselves identified to firms engaging in direct mail solicitation with respect to products or services related to the activity for which the individual has obtained a licence or permit. The interest of the government in providing such information, of course, is simply to generate revenue. In cases such as this, we see no reason, in principle, to prohibit revenue-generating activity of this kind. The privacy interests of the individuals involved are protected by ensuring that communication of their name and address is something to which they have willingly agreed.

RECOMMENDATIONS

Our recommendations with respect to the provision of mailing list information by government institutions are the following:

1. Governmental institutions which maintain public records containing the names and addresses of individuals should be encouraged to devise procedures whereby such individuals could indicate on the public record in question that they do not wish to have their names included on mailing lists compiled from those records.
2. Governmental institutions which possess records containing names and addresses of individuals which would not normally be made available to the public should be permitted to sell or supply name and address information for mailing list purposes only if the individuals in question have given their consent to the communication of this information for such purposes.

CHAPTER 37 NOTES

- 1 See generally, Alan F. Westin, Databanks in a Free Society (New York: Quadrangle/The New York Times Book Company, 1972) 161-67.
- 2 39 U.S.C. 3010.
- 3 Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: USGPO, 1977) 127-29; hereafter cited as PPSC Report.
- 4 Ibid., 130.
- 5 U.S.C. 552a(n).
- 6 In Getman v. NLRB, 450 F. 2d 670 (D.C. Cir., 1971), the D.C. Court of Appeals allowed a law professor access for research purposes to a list of names of those who had participated in an election supervised by the National Labour Relations Board. However, in Wine Hobby U.S.A. Inc. v. IRS, 502 F. 2d 133 (3d Cir., 1974), a request for a government list of persons making wine for personal consumption for the purpose of contacting them for commercial mail advertising was denied on the grounds that disclosure of names and addresses would be a "clearly unwarranted invasion of privacy" and therefore the information was exempt under the FOIA: PPSC Report, 131.
- 7 PPSC Report, 132.
- 8 Ibid., 153.
- 9 Privacy Project Task Group, Report of the Privacy and Security Survey of Information on Individuals, Project #628, August 13, 1975. The ministries surveyed were: Education, Health, Labour, Revenue, Consumer and Commercial Relations, Community and Social Services, Transportation and Communications, the Solicitor General and Colleges and Universities. The mailing list data were: Health, 1; Consumer and Commercial Relations, 3; Colleges and Universities, 2; Education, 2.
- 10 M. Brown, B. Billingsley and R. Shamai, Privacy and Personal Data Protection (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980) 635-6.

Transborder Data Flows

In recent years, the movement of computerized personal data across national borders has become a matter of international concern. The implications of transborder data flows for the protection of privacy are perhaps self-evident. Once personal data is transferred to another jurisdiction for processing and storage it becomes subject to the laws of that country. The country in which the data originated loses control over the possible uses to be made of the data[1].

The enactment of data protection schemes has led to extensive consideration of these problems in Europe. A number of European countries appear to be moving toward restricting the flow of personal data beyond their borders. The OECD has drafted guidelines on transborder data flows and the protection of privacy, and it has recommended adoption of these guidelines by its member countries to ensure uniformity of data protection laws[2]. In Canada, attention was drawn to this issue in 1972 by a federal government task force on computers and privacy[3]. The task force noted that a growing volume of personal data relating to Canadians was being transmitted for processing and storage outside Canadian borders, chiefly in the United States. The transferred data had been collected by the private sector, and concerned the credit-worthiness, medical histories, travel arrangements and financial positions of Canadians[4].

Although the issue of privacy protection may have given rise to some of the initial concerns relating to transborder data flows, public discussion in Canada and elsewhere has more recently expanded to include a consideration of the economic, social and political aspects of this development[5]. Some of these concerns were expressed by the former federal Minister of Science and Technology, J. Hugh Faulkner, who stated in 1977 that the transfer of computing activities outside of Canada associated with increasing transborder data flows

creates the potential of growing dependence, rather than interdependence, the loss of employment opportunities, an addition to balance of payments problems, the danger of loss of legitimate access to vital information and the danger that industrial and social development will largely be governed by the decisions of interest groups residing in another country[6].

The issues raised by the increasing volume of transborder data flows were also examined by a committee established by the Canadian government which recommended in 1979 that Canada take immediate action to regulate transborder data flows "to ensure that we do not lose control of information vital to the maintenance of national sovereignty"[7].

Our particular concerns, of course, relate to the privacy protection implications of the data processing practices of the Ontario government. Accordingly, it is of interest that it is the policy of the Ontario government that all of its data processing activity and data storage must take place in Canada[8]. This policy is meant to ensure that provincial governmental institutions do not establish automated files or data bases about Canadian citizens (and particularly Ontario residents) outside the jurisdiction of Canadian law, and to preserve business opportunities for the Canadian information processing industry. Although the policy specifically permits ministries to apply to Management Board for an exemption from this requirement, no such application has been made.

There is, on the other hand, no overall policy of the Ontario government relating to transborder exchanges of personal data held by government; decisions to engage in such transfers are the responsibility of each ministry. In the course of administering various government programs, such exchanges do, in fact, occur. A number of illustrations of this phenomenon came to the attention of our research staff. For example, public welfare roster information is shared among Ontario, other provinces, and U.S. border states in individual cases where it comes to the attention of one jurisdiction that a person might be receiving assistance from another jurisdiction. Information may also be shared on a case-by-case basis between Ontario and other jurisdictions where there are reciprocal agreements with respect to the enforcement of family support obligations. Similarly, there is some exchange of adoption records with other jurisdictions in special circumstances. This has occurred, for example, to assist an adoptee who has legitimate reasons to inquire into his family origins, such as a need to know particular medical or other family information. Such exchanges take place only on a case-by-case basis. Access to sealed adoption records can only be obtained by a court order or on the written direction of the Director of the Children's Services Division of the Ministry of Community and Social Services[9].

Cooperative information sharing also occurs among law enforcement authorities in neighbouring jurisdictions. In an earlier chapter, a description was given of the operations of the Canadian Police Information Centre (CPIC), which is linked internationally with the NCIC in Washington, D.C. and with INTERPOL.

The operation of CPIC is the responsibility of the RCMP. Information relating to violations of Ontario statutes is available on CPIC, but usually to Ontario forces only; it is not normally the subject of transborder information exchanges. Basic driver licensing and vehicle registration information about Ontario residents is shared with other provincial law enforcement agencies through CPIC. Information arising from violations of federal statutes, including the Criminal Code, is available to law enforcement agencies on an international basis through the CPIC system.

Although our investigation of the privacy protection implications of transborder data flows must be considered to be rather preliminary in nature, it appears that current practice of the Ontario government in this regard is consistent with privacy protection considerations. However, it is our view that the privacy protection implications of transborder data storage and exchanges are matters that should be subject to the continuing scrutiny of the proposed Data Protection Authority and the Director of Fair Information Practices. Further, we have previously recommended that the Data Protection Authority be assigned a responsibility to examine and make recommendations with respect to the personal data-handling practices of private sector organizations. A consideration of the privacy protection implications of transborder data flows should constitute one aspect of the inquiries undertaken by the DPA in exercising this responsibility.

RECOMMENDATIONS

In summary, then, we recommend that transborder storage and transfer of personal data be the subject of study by the Data Protection Authority with a view to making such recommendations as may be appropriate in the light of privacy protection considerations.

CHAPTER 38 NOTES

- 1 This was recently brought home forcefully to Swiss authorities when the United States Internal Revenue Service expressed an interest in gaining access, using its subpoena powers if necessary, to Swiss banking data stored in computers in Ohio. See Joseph E. Shickich, Jr., "Transborder Data Flow," Law and Computer Technology, 3rd Quarter (1978) 62.
- 2 Draft Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris: Organization for Economic Co-Operation and Development, 1979).
- 3 Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972).
- 4 Ibid., 170.
- 5 See, for example, The Vulnerability of Computerized Society (Stockholm: Ministry of Defence, 1978) summarized in Transnational Data Report, Vol. 1, No. 5 (November 1978).
- 6 J.H. Faulkner, address at the official opening of the International Federation for Information Processing, Toronto, Ontario (August 1977) quoted in Peter Robinson, "Transborder Dataflow -- A Canadian Perspective," Information Privacy, Vol. 2, No. 2, (March 1980) 55, cited hereafter as Robinson.
- 7 Canadian Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty, Telecommunications and Canada (Ottawa: Department of Supply and Services, 1979), quoted in Robinson, 57. The proposed revisions to the Bank Act (Bill C-6) tabled in the House of Commons in April 1980 contain provisions to ensure that the federal government will be able to gain access to Canadian bank records for the purposes of regulation and enforcement of the Bank Act. Section 157.4 requires Canadian banks to retain in Canada all records that are subject to inspection by government authorities.
- 8 Information about transborder data flows relating to records containing personal data held by the Ontario government has been supplied by B.G. Cook, Senior Management Policy Advisor, Management Technology Branch, Management Board of Cabinet, in a letter to the Commission dated March 22, 1979.
- 9 This is expressly provided for in The Child Welfare Act, 1978, S.O. 1978, c. 85, s. 74.

Freedom of Information and Individual Privacy

In the preceding chapters of this report, we have recommended the enactment of a comprehensive freedom of information law which will provide a secure legal foundation for the public's right to obtain information about governmental institutions. As well, we have recommended the adoption of a comprehensive data protection law which ensures that governmental institutions engaging in the collection, storage, use and dissemination of personal information will adopt practices which will afford adequate protection to the personal privacy of individuals about whom such records are maintained. Both these schemes draw support from the traditional view taken in democratic societies with respect to the relationship between government and the governed. Public institutions are required to conduct their affairs in such a manner as to facilitate public accountability. Scrutiny of public institutions by individual citizens is encouraged, while scrutiny of the private lives of citizens by governmental institutions is discouraged. The private lives of individual citizens are protected by ensuring that proper limitations on the use of surveillance of individual citizens are observed by government.

In this sense, both schemes derive from a consistent philosophical position. It is evident, however, that the public right to know will, on occasion, collide with the right of individuals to control the flow of personal information concerning themselves. At various points in this report, we have drawn attention to the need to effect an appropriate reconciliation between these two interests in cases of conflict. In this chapter, we attempt to draw together the various threads of this problem and indicate the nature of the reconciliation we recommend.

In Chapter 1 of this report, we indicated that the principal points of conflict between freedom of information (FOI) and privacy protection schemes arise with respect to the following matters:

1. How is the principle of the public right to know to be reconciled with the protection of privacy where access is sought to government documents containing personal information about persons other than the individual making the request?

2. What controls, if any, are there to be on the disclosure of personal information which may be exempt from disclosure under the FOI scheme but which, nonetheless, the government may be willing to disclose? To put the question differently, should a privacy exemption be "discretionary" or "mandatory"?
3. If the privacy scheme embodies as one of its privacy protection devices the granting of a right of access to individuals to government documents containing information about them (a subject access scheme), are there exemptions to this principle of access and, if so, how do they relate to the exemptions under the FOI scheme?
4. Are the procedural mechanisms, administrative arrangements, and appeal mechanisms with respect to the FOI and subject access schemes properly integrated?

We will consider each of these areas in turn.

A. THE PERSONAL PRIVACY EXEMPTION TO THE FOI SCHEME

Many government records contain personal information about identifiable individuals. In order to ensure that the FOI scheme does not become an instrument for the invasion of personal privacy, some exemption must be made from the general rule of access for records containing sensitive personal information.

As we indicated in our discussion of these matters in Volume 2, Chapter 14, we do not believe it would be satisfactory simply to exempt all records containing personal information from the freedom of information law. The privacy protection interest is, of course, an important one but we do not think that it should be treated as an absolute. On occasion, the interest of an individual in preserving personal privacy must yield to the public interest in being able to subject the conduct of public affairs to scrutiny. Accordingly, it was necessary for us to develop recommendations which would establish an appropriate mechanism for striking a balance between these two competing interests. Under the U.S. Freedom of Information Act, the device established for these purposes is to be found in the exemption relating to records containing personal information which, if disclosed, would constitute a "clearly unwarranted invasion of privacy." Similar provisions have been included in freedom of information laws of other jurisdictions and in proposals made in Australia. Our view is that a test of this kind is undesirably vague and imprecise in its interpretation. Therefore, we have recommended the adoption of a privacy protection exemption which we believe will offer clearer

guidance as to the kinds of considerations to be taken into account in making a determination whether to disclose a record containing personal information.

In our earlier discussion, we identified the following as the desirable features of a personal privacy exemption to the FOI scheme:

- . the statute should, to the greatest extent possible, clearly identify situations in which there is an undeniably compelling interest in access;
- . for those cases not resolved by such explicit provisions, a general balancing test should be stated with some indication of the factors to be weighed in an application of the test to a particular document;
- . as part of the criteria set forth for the application of the balancing test, personal information generally regarded as particularly sensitive should be identified in the statute and made the subject of a presumption of confidentiality.

It is unnecessary to repeat here the detailed recommendations we have made with respect to each of these features of the proposed exemption. Speaking generally, the situations in which disclosure is encouraged are those in which the basic purpose of the freedom of information scheme -- facilitating public scrutiny of government conduct -- will be furthered by disclosure. As the personal information subject to the request becomes more sensitive in nature, however, the effect of the proposed exemption is to tip the scale in favour of non-disclosure. Although the exempting provision is, as a result, rather complex in its design, we believe that a more elaborately structured balancing test of this kind will allow easier interpretation and application than does its U.S. counterpart.

B. THE MANDATORY NATURE OF THE FOI PRIVACY EXEMPTION

As a general rule, we have recommended that the exemptions to the FOI scheme be "permissive" in nature in the sense that even though a particular record may be exempt from the general rule of access, the government retains a discretion to disclose the document if it wishes to do so. It is desirable to confer such a discretion on the government, for there may be many situations in which an exempt document could be disclosed without any prejudice to a legitimate government interest in confidentiality. However, we take a different view of the nature of the exemption relating

to records containing sensitive personal information. It is our view that where records of this kind are exempt because disclosure would constitute an invasion of privacy, the governmental institution in question should be under an obligation to refuse to disclose the record. Therefore, we have recommended that the personal privacy exemption be "mandatory" in nature.

We have further recommended that individual data subjects should be given, to the extent practicable, an opportunity to participate in decisions made to release documents containing personal information. Under our proposals, governmental institutions are encouraged to give notice to individuals of proposed disclosures. Data subjects who are concerned that a proposed disclosure is not authorized by the freedom of information scheme may protest the disclosure to the Director of Fair Information Practices and, on appeal, to the Fair Information Practices Tribunal. Both the director and the tribunal would be empowered to order that the document not be released.

C. INTEGRATION OF THE ACCESS RIGHTS AND EXEMPTIONS OF THE TWO SCHEMES

A freedom of information law provides a broad general right of access to government documents. Privacy protection schemes, and in particular our own proposed scheme, typically provide individuals with rights of access to government records containing personal information pertaining to themselves. When the two schemes are adopted in tandem, care must be taken to ensure that the operation of the access rights and the exemptions under each scheme intersect appropriately with each other. As we have indicated elsewhere in this report, integration of these aspects of the two schemes has proved to be troublesome in the U.S. experience under the Freedom of Information Act and the Privacy Act of 1974.

In order to explain the integration which we propose, it will be useful to refer briefly to the nature of the difficulties which have arisen in the United States. First, it must be noted that the right of access conferred on individuals under each of the two schemes differs in important respects. The U.S. Freedom of Information Act, broadly speaking, provides rights of access to any accessible record. If the individual making the request can reasonably describe the record in question, and if the record is not covered by one of the exempting provisions, the agency possessing the record must disclose it. The exemptions from the general rule of access are defined in terms of particular kinds of documents or particular kinds of information.

The access rights conferred by the U.S. Privacy Act of 1974 are designed in a rather different fashion. In essence, individual data subjects are granted rights of access with respect to information stored in "systems" of personal data or what might be referred to for purposes of discussion as "data banks." In order to constitute a system or data bank for these purposes, the collection of records must be retrievable on the basis of a person's name or some other identifier. The access rights conferred by the act extend only to records contained in such systems. Further, the exemptions to the general rule of data subject access are also cast in terms of "systems." Thus, entire data banks, rather than types of documents or information, are excluded from the rights of access conferred by the scheme. A further difference between the freedom of information and privacy schemes, of course, is that the privacy scheme couples access rights with correction rights. Thus, if an individual is entitled to access to information contained in a non-exempt data bank, he is also entitled to seek correction of material in the record which he believes to be erroneous.

The data subject rights conferred by the two schemes, then, are dissimilar in a number of important respects. An individual seeking access to government records containing personal information might prefer to pursue rights of access under the Freedom of Information Act rather than the Privacy Act in two kinds of situations. First, the individual might wish to obtain access to material not contained in a data bank. Records containing personal information will often be contained in record systems which do not use personal identifiers as a key to retrieval. (For example, information may be filed according to the date of the document, or on the basis of geographic location, project numbers or job descriptions.) Access to such material could only be obtained under the Freedom of Information Act. Second, an individual would prefer to exercise freedom of information rights in the case where the information is contained in a data bank which has been exempted from the subject access provisions of the Privacy Act. Inasmuch as the freedom of information exemptions are based on document or information types, there arise situations in which information contained in an exempt data bank will be subject to a right of access under the Freedom of Information Act.

A number of difficulties and anomalies have arisen in the experience of U.S. federal agencies responding to requests from individuals to obtain access to personal records. Frequently, of course, the individual making the request will not appreciate the subtleties of the distinctions between the operations of these statutes and, indeed, may not refer to either statute by name in making a request. Some federal agencies have treated such requests as invoking rights under both statutes and have responded

to them on this basis. Others have assumed that the Privacy Act is the exclusive vehicle for handling requests by data subjects for access to their files. The curious result of this practice is that third parties seeking access to personal information about an individual under the Freedom of Information Act may have greater rights of access to the file than would the data subject himself under the Privacy Act. Many agencies have adopted a further alternative method of dealing with these requests. Data subject requests are treated as requests under the Privacy Act but in cases where access is to be denied, individual requesters are informed of the existence of the Freedom of Information Act and its possible implications for access to the record in question.

Our proposals have been fashioned in such a way as to avoid these problems. Our recommendations are based on two decisions on matters of policy relating to the interaction of the schemes. First, it is our view that the broader rights of subject access of the kind conferred by the Freedom of Information Act are preferable to the more limited rights of access conferred by the Privacy Act. Accordingly, some place must be found in our proposed legislation for the granting of subject access rights to all reasonably accessible records containing personal information. Second, it is our view that correction rights should pertain to records made available under this broad right of access. Individuals should be entitled to seek correction of records containing personal information even though the record is not contained within a "system" of personal records or data bank. We note that similar recommendations have been made by the U.S. Privacy Protection Study Commission in its review of the operation of the Privacy Act of 1974.

An extended scheme of access and correction rights of this kind could be embodied either in a freedom of information law or in a privacy protection scheme. The Nova Scotia Freedom of Information Act, for example, confers rights of data subject access and correction. However, we think that it would be desirable to locate the subject access scheme within the proposed privacy protection legislation for three reasons. First, the exemptions typically contained in a freedom of information law are not tailored precisely to the needs of a subject access scheme. Accordingly, it is preferable to include subject access rules in a separate statute or at least in a separate part of a general fair information practices law. Second, the data protection law which we have proposed establishes certain mechanisms which will lead to effective privacy protection planning in the establishment of new data systems. We believe that planning for the establishment of satisfactory data subject and access rights should form part of that process. Third, data subject access and correction rights are conferred as part of an interrelated set of measures designed to protect personal privacy; therefore, there is some logic in

including subject access provisions in the same enactment as these other privacy protection devices.

For these reasons, then, we have recommended that subject access and correction rights pertaining to reasonably accessible records containing personal information should be conferred as part of our proposed data protection law. If such a law is enacted so as to take effect at the same time as a freedom of information law enacted in accord with our proposals, it follows that it would be acceptable to stipulate that the privacy protection scheme is to constitute the exclusive vehicle for the exercise of data subject rights of access. If a data protection law were not to be enacted at the same time as a freedom of information law, however, it would be necessary to reconsider the question of including data subject access and correction rights within the freedom of information scheme. As we have indicated elsewhere in this report, the objective of securing rights of access to files pertaining to individuals is one of the primary objectives of freedom of information legislation. The right of subject access could be deleted from a freedom of information law, in our view, only if it were satisfactorily established in companion privacy protection legislation.

With specific reference to the matter of exemptions, we believe that some, but not all, of the freedom of information exemptions are appropriate in a subject access scheme. The freedom of information exemptions which, we believe, are equally appropriate in the subject access scheme relate to the following matters:

- . Cabinet documents;
- . law enforcement;
- . international relations and national defence;
- . information received in confidence from other governments;
- . information creating unfair advantage or harm to negotiations;
- . solicitor-client privilege.

In addition, we believe that the following exemptions from subject access are necessary:

- information whose disclosure would constitute an unwarranted invasion of another individual's personal privacy;
- evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for appointment to public or judicial office or for the awarding of government contracts and other benefits, but only to the extent that the disclosure of such material would reveal the identity of the source who furnished the information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the enactment of this legislation, under an implied promise that the identity of the source would be held in confidence;
- medical information whose disclosure would prejudice the health of the data subject;
- correctional records whose disclosure could reasonably be expected to (1) seriously disrupt an individual's institutional, parole or mandatory supervision program; (2) reveal information supplied on the promise of confidentiality, express or implied; or (3) result in physical or other harm to that individual or any other person.
- research and statistical records.

Our reasons for suggesting the adoption of each of these exemptions are set out in Chapter 33 of this report.

D. INTEGRATION OF PROCEDURAL MECHANISMS, ADMINISTRATIVE ARRANGEMENTS AND APPEAL MECHANISMS

In making our recommendations for the proposed freedom of information law and the proposed data protection law, we have attempted to ensure that the procedural, administrative and appeal mechanisms established under each scheme are generally parallel. We believe that the independent body offering authoritative interpretations of the exemptions from the general rule of access in the freedom of information scheme should also be the authoritative source of interpretation with respect to the exempting provisions of the data protection law. Since, as we have indicated, in many instances the data protection scheme exemptions will be the same as those in the freedom of information law, it would be undesirable to devise a system whereby differing interpretations might be

given to the same exemptions. Accordingly, we have recommended that individuals exercising rights conferred either by the freedom of information law or the data protection law be permitted to seek the intervention of the Director of Fair Information Practices and, on appeal, the Fair Information Practices Tribunal.

The procedures established under both schemes for the handling of requests made by individuals to obtain access to government documents are also parallel. Similar recommendations have been made with respect to such matters as the form of the request, fees, time limits, and the requirements of adequate notice of reasons for denying requests. If subject access rights are conferred only under the data protection scheme, it is not essential that the procedural mechanisms be precisely parallel; it is our view, however, that the procedural mechanisms and safeguards appropriate in the freedom of information context are also appropriate in the context of data subject requests made under the data protection law.

Mention must also be made of the administrative arrangements concerning the implementation of these two schemes. In our discussions of these matters, we have resisted making explicit recommendations with respect to the administrative machinery which should be established in each institution for the handling of freedom of information act requests or the exercise of rights under the data protection scheme. We have limited our proposals to a recommendation in each context that a particular official be assigned the responsibility for ensuring the implementation of each scheme within each institution subject to the legislation. As a general rule, we believe that it would be useful to ensure that both functions are performed by the same administrative unit. In the context of relatively small institutions, it may be possible that one public servant could perform both tasks. However, we do not feel that it would be appropriate for the Commission to attempt to make detailed recommendations as to the most effective manner of structuring internal administrative processes for implementing these schemes.

Finally, attention must be drawn to the recommendations relating to the Data Protection Authority (DPA), a body whose functions are restricted to the operation of the data protection law. As we have explained at length in earlier chapters of this report, it is our view that in addition to the conferral of various rights on data subjects, a data protection law should establish a mechanism to facilitate the implementation of fair information practices in the design and establishment of government data banks. We propose to assign responsibilities of this kind to the Data Protection Authority rather than to the Director of Fair Information Practices or the Fair Information Practices

Tribunal. The functions of the DPA are, we believe, different from those assumed by the director and the tribunal. We recommend that the DPA's role be to engage in a detailed application of statutory data management standards to specific data banks. This will require considerable expertise in information systems design with respect to such matters as systems security. The DPA will facilitate, through its planning and approval responsibilities, the establishment of data systems which will operate in accordance with the data management standards imposed in the data protection scheme. The director and the tribunal, on the other hand, will perform the function of adjudicating disputes arising between individuals making requests under the freedom of information law or exercising privacy protection rights under the data protection law. The DPA plays no role in the implementation of the freedom of information scheme for the obvious reason that data management standards have not been recommended with respect to information systems that are subject merely to the general requirements of the freedom of information law. Statutory standards for the management of data systems containing personal information have been recommended in order to ensure that such systems are operated in a fashion consistent with privacy protection considerations.

In summary, then, we believe that our recommendations establish a satisfactory mechanism for achieving an appropriate balance between the public right to know and the interest of the individual in personal privacy. As well, we believe that our recommendations effectively integrate the various features of our proposed freedom of information and data protection schemes.

Appendix: Statutory Material

PROTECTION OF PERSONAL INFORMATION

Interpretation

49. In this Part,

“administrative purpose”, in relation to the use of a record regarding an individual, means the use of that record in a decision making process that relates directly to that individual;

“appropriate Minister”, in relation to a government institution, means the member of the Queen’s Privy Council for Canada presiding over that institution or through which that institution reports to Parliament;

“derivative use” means a use of a record for a purpose that, in the opinion of the appropriate Minister, is consistent with the use for which it was compiled, and any use of a record that is not a derivative use is a “non-derivative use”;

“designated Minister”, in relation to any provision of this Part, means such member of the Queen’s Privy Council for Canada as is designated by the Governor in Council to act as the Minister for the purposes of that provision;

“federal information bank” means a store of records within the control of a government institution where any of the records comprised therein are used for administrative purposes;

“government institution” means any department of the Government of Canada and any board, commission, body or office listed in the schedule;

“individual” means a Canadian citizen or an individual lawfully admitted to Canada for permanent residence;

“information bank” means a collection or grouping of personal information recorded in any form, that is within the control of a government institution and that has been collected from an individual or individuals or a corporation or institution;

“personal information” means information respecting an individual if that informa-

tion contains the individual’s name or if the individual’s identity is readily ascertainable from that information;

“record” means an item, collection or grouping of personal information recorded in any form.

Application

50. (1) This Part applies to all federal information banks.

(2) Nothing in this Part authorizes the release to any person or the examination by any person of information about that person contained in a federal information bank in contravention of any agreement between the Government of Canada or a Minister of the Crown in right of Canada and the government of a province or a Minister of the Crown in right of a province under which information was made available in confidence for inclusion in the information bank.

Federal Information Bank Index

51. (1) The designated Minister shall cause to be published on a periodic basis not less frequently than once each year, a publication setting forth the name or identification of each federal information bank, the type of records stored therein, the derivative uses of those records and such other information as is prescribed by the regulations.

(2) The designated Minister shall cause the publication referred to in subsection (1) to be made available throughout Canada in a manner commensurate with the principle that every individual is entitled to reasonable access thereto in order to be informed of the contents thereof.

Access to and Use of Records

52. (1) In furtherance of the principle enunciated in paragraph 2(b) that the privacy of individuals and their right of access to records containing personal information concerning them for any purpose including the purpose of ensuring accuracy and completeness, should be protected to the greatest

extent consistent with the public interest, every individual is entitled to

(a) ascertain what records, concerning that individual that are used for administrative purposes are contained in federal information banks named or otherwise identified in the publication referred to in subsection 51(1);

(b) ascertain the uses to which such records have been put since the coming into force of this Part;

(c) examine each such record or a copy thereof whether or not that individual provided all or any of the information contained in the record;

(d) request correction of the contents of any such record where that individual believes there is an error or omission therein; and

(e) require a notation on any such record of a requested correction therein where the contents of such record are not amended to reflect the requested correction.

(2) Every individual is entitled to be consulted and must consent before personal information concerning that individual that was provided by that individual to a government institution for a particular purpose is used or made available for use for any non-derivative use for an administrative purpose unless the use of that information for that non-derivative use is authorized by or pursuant to law.

(3) Where notice in writing is given to an individual that personal information described in subsection (2) concerning that individual is proposed to be used for a purpose specified in the notice that is a non-derivative use for an administrative purpose, that individual shall be deemed to have been consulted and to have consented to the use of the information for the specified purpose unless written notice to the contrary is given by that individual, in a prescribed manner and within a prescribed time specified in the notice.

(4) Where an individual is denied any right provided by subsection (1) on the ground that, by virtue of section 54 or 55, subsection (1) or a provision thereof does not apply in the circumstances, the appropriate Minister shall advise the individual in writing of the particular ground on which the right is denied.

Exemptions

53. The appropriate Minister in relation to a government institution that has control of a federal information bank may, with the approval of the Governor in Council, by order specifying the provision of this section that is the basis for the restriction or exemption, restrict the information relating to that information bank that is required to be published in the publication referred to in subsection 51(1) and provide that subsection 52(1) or any provision thereof specified in the order does not apply to records contained therein where, in the opinion of the Minister, disclosure of information contained in the information bank or relating thereto

(a) might be injurious to international relations, national defence or security, or federal-provincial relations; or

(b) would be likely to disclose information obtained or prepared by any government institution or part of a government institution that is an investigative body

(i) in relation to national security,

(ii) in the course of investigations pertaining to the detection or suppression of crime generally, or

(iii) in the course of investigations pertaining to particular offences against any Act of Parliament.

54. The appropriate Minister in relation to a government institution that has control of a federal information bank may provide that subsection 52(1) or any provision thereof specified by him does not apply in respect of a record or part thereof concerning an individual in the information bank where, in the opinion of the Minister, knowledge of the

existence of the record or of information contained therein

(a) might be injurious to international relations, national defence or security or federal-provincial relations;

(b) would disclose a confidence of the Queen's Privy Council for Canada;

(c) would be likely to disclose information obtained or prepared by any government institution or part of a government institution that is an investigative body

(i) in relation to national security,

(ii) in the course of investigations pertaining to the detection or suppression of crime generally, or

(iii) in the course of investigations pertaining to the administration or enforcement of any Act of Parliament;

(d) might, in respect of any individual under sentence for an offence against any Act of Parliament

(i) lead to a serious disruption of that individual's institutional, parole or mandatory supervision program,

(ii) reveal information originally obtained on a promise of confidentiality, express or implied, or

(iii) result in physical or other harm to that individual or any other person;

(e) might reveal personal information concerning another individual;

(f) might impede the functioning of a court of law, or a quasi-judicial board, commission or other tribunal or any inquiry established under the *Inquiries Act*; or

(g) might disclose legal opinions or advice provided to a government institution or privileged communications between lawyer and client in a matter of government business.

55. (1) The appropriate Minister in relation to a government institution that has control of a federal information bank may, by order, provide that subsection 52(1) or

any provision thereof specified in the order does not apply in respect of the information bank where,

(a) no order has previously been made under this subsection in respect of the information bank; and

(b) in the opinion of the Minister, the public benefit to be derived from the application of that subsection or the provisions thereof specified in the order in respect of the information bank is outweighed by the costs that would be incurred in applying that subsection or those provisions thereto.

(2) Where an order of a Minister made under subsection (1) remains in force, with or without amendment, in respect of a particular federal information bank for more than two years, records stored in the information bank may not, after the expiration of two years from the day on which such order was made, be used for administrative purposes until the order is revoked.

Coordination of Information Banks

56. (1) The designated Minister shall

(a) cause to be kept under review the manner in which federal information banks are maintained and managed to ensure compliance with the provisions of this Part and regulations made thereunder relating to access by individuals to records concerning them in those information banks;

(b) ensure the availability throughout Canada of the publication referred to in subsection 51(1);

(c) prescribe such forms as may be required for the operation of this Part and regulations made thereunder; and

(d) cause to be prepared and distributed to government institutions guidelines concerning the operation of this Part and regulations made thereunder.

(2) In order to coordinate the collection for, and the retention, use and storage of information in, information banks within the control of government institutions and to eliminate wherever possible any unnecessary collection of information for storage in such

information banks, the designated Minister shall cause to be kept under review the utilization of existing information banks and proposals for the creation of new information banks or the substantial modification of existing ones and shall make such recommendations as he considers appropriate to appropriate Ministers with regard to information banks that, in his opinion, are under-utilized or the existence of which can be terminated.

(3) For the purposes of coordinating the collection of information for storage in information banks within the control of government institutions, eliminating, wherever possible, any unnecessary collection of information for such storage and increasing utilization of information already stored in such information banks, no new information bank shall be established and no existing information bank shall be substantially modified without the approval of the designated Minister or otherwise than in accordance with any term or condition on which any such approval is given.

Privacy Commissioner

57. The Minister of Justice, on the recommendation of the Chief Commissioner of the Canadian Human Rights Commission established by section 21, shall designate a member of that Commission to act as Privacy Commissioner.

Investigations

58. (1) The Privacy Commissioner shall receive, investigate and report on complaints from individuals who allege that they are not being accorded the rights to which they are entitled under this Part in relation to personal information concerning them that is recorded in a federal information bank.

(2) Nothing in this Part precludes the Privacy Commissioner from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorized by the complainant to act on behalf of the complainant.

(3) Every investigation by the Privacy Commissioner shall be conducted in private.

(4) It is not necessary for the Privacy Commissioner to hold any hearing and no person is entitled as of right to be heard by the Privacy Commissioner but if at any time during the course of an investigation it appears to the Privacy Commissioner that there may be sufficient grounds for making a report or recommendation that may adversely affect any person or any government institution concerned, the Privacy Commissioner, before completing the investigation, shall ensure that reasonable measures have been taken to give that person or government institution a full and ample opportunity to answer any adverse allegation or criticism and to be assisted or represented by counsel for that purpose.

(5) The Privacy Commissioner has, in relation to the carrying out of an investigation, the powers of a Human Rights Tribunal under Part III and, in addition to those powers, may, subject to such limitations as the Governor in Council in the interest of national defence or security may prescribe, enter any premises occupied by any government institution concerned in the investigation and carry out therein such inquiries as the Commissioner sees fit.

59. (1) If, at the conclusion of an investigation, the Privacy Commissioner finds that the complainant is not being accorded a right to which he is entitled under this Part in relation to personal information concerning him that is recorded in a federal information bank, the Commissioner shall provide to the appropriate Minister in relation to the government institution that has control of that information bank a report containing

(a) the findings of the investigation and any recommendations that the Commissioner considers appropriate; and

(b) where appropriate, a request that, within a time specified therein, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(2) The Privacy Commissioner shall report to the complainant, or to a person authorized by the complainant to act on behalf of the complainant, the findings of the investigation of a complaint but where, pursuant to paragraph (1)(b), a notice has been requested of action taken or proposed to be taken in relation to recommendations of the Commissioner arising out of the complaint, no report shall be made under this subsection until the expiration of the time within which that notice is to be given to the Commissioner.

(2.1) Where, pursuant to paragraph (1)(b), a notice has been requested of action taken or proposed to be taken in relation to recommendations of the Privacy Commissioner arising out of a complaint and no such notice is received by the Commissioner within the time specified therefor or the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Commissioner shall so advise the complainant in his report to the complainant under subsection (2) and may include in the report such comments on the matter as he thinks fit.

(3) Any report made by the Privacy Commissioner under subsection (1), together with any notice given to the Commissioner in response thereto, may be included in a report made pursuant to subsection 60(1), and notice of each case in which a notice has been requested by the Privacy Commissioner, pursuant to paragraph (1)(b), of action taken or proposed to be taken and in which no such notice is received by him within the time specified therefor or in which the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time shall be included in a report made pursuant to subsection 60(1).

(4) In a report made under this section, the Privacy Commissioner shall take every reasonable precaution to avoid revealing any personal information and any matter referred to in subsection 60(2).

60. (1) The Privacy Commissioner shall, within five months after the 31st day of December in each year, and at such other times as are appropriate, transmit to the Minister of Justice a report on the activities of the office since the date of the last such report and the Minister shall cause each such report to be laid before Parliament within fifteen days after receipt thereof or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

(2) In any report made under this section, the Privacy Commissioner shall take every reasonable precaution to avoid revealing personal information and any matter the disclosure of which

(a) might be injurious to international relations, national defence or security or federal-provincial relations;

(b) would disclose a confidence of the Queen's Privy Council for Canada;

(c) would be likely to disclose information obtained or prepared by any government institution or part of a government institution that is an investigative body

(i) in relation to national security,

(ii) in the course of investigations pertaining to the detection or suppression of crime generally, or

(iii) in the course of investigations pertaining to particular offences against any Act of Parliament;

(d) might, in respect of any individual under sentence for an offence against any Act of Parliament,

(i) lead to a serious disruption of that individual's institutional, parole or mandatory supervision program,

(ii) reveal information originally obtained on a promise of confidentiality, express or implied, or

(iii) result in physical or other harm to that individual or any other person;

(e) might impede the functioning of a court of law, or a quasi-judicial board,

commission or other tribunal or any inquiry established under the *Inquiries Act*; or
(f) might disclose legal opinions or advice provided to a government institution or privileged communications between lawyer and client in a matter of government business.

Special Studies

61. (1) The Privacy Commissioner shall carry out or cause to be carried out such studies as may be referred to the Privacy Commissioner by the Minister of Justice concerning the extension of the principle described in paragraph 2(b) and the rights to which individuals are entitled under this Part to stores of records within the control of bodies, other than government institutions, that come within the legislative authority of Parliament, and the Privacy Commissioner shall report thereon to the Minister of Justice from time to time.

(2) The Minister of Justice shall cause each report by the Privacy Commissioner under subsection (1) to be laid before Parliament within fifteen days after receipt thereof or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

Regulations

62. (1) The Governor in Council may make regulations

(a) prescribing classes of information to be set forth in the publication referred to in subsection 51(1);

(b) prescribing the procedure to be followed in permitting an individual to examine personal information concerning that individual in any record or class of records contained in a federal information bank;

(c) prescribing the procedure to be followed where an individual wishes to request correction of personal information concerning that individual in any record or

class of records contained in a federal information bank;

(d) prescribing any special procedures or restrictions deemed necessary with regard to examination of medical records of an individual, including psychological reports concerning that individual, and, if deemed appropriate, procedures that would preclude examination of such records and reports by the individual where, in the opinion of a duly qualified medical practitioner, examination thereof by the individual would be contrary to the best interests of the individual;

(e) prescribing any special procedures to be followed by a government institution in obtaining personal information for inclusion in a federal information bank;

(f) prescribing procedures to be followed by the Privacy Commissioner in conducting investigations pursuant to this Part;

(g) providing for the management and surveillance of records of any government institution to promote the protection of individual privacy and to ensure that the provisions of this Part are complied with;

(h) prescribing a schedule of fees for examination of records; and

(i) prescribing anything that, pursuant to any provision of this Part, is to be prescribed by regulation.

(2) The Governor in Council may, by order, amend the schedule by adding thereto any department, board, commission, body or office of the Government of Canada.

(3) No schedule of fees prescribed pursuant to paragraph (1)(h) may provide for a fee for the examination of any record where, by or pursuant to any enactment or any agreement to which Her Majesty in right of Canada or an appropriate Minister is a party, the right of examination thereof is to be provided without fee or charge.

§ 552a. Records maintained on individuals

(a) Definitions

For purposes of this section—

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13; and

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

(b) Conditions of disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

(11) pursuant to the order of a court of competent jurisdiction.

(c) Accounting of certain disclosures

Each agency, with respect to each system of records under its control shall—

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to records

Each agency that maintains a system of records shall—

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and—

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either—

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in

accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) Agency requirements

Each agency that maintains a system of records shall—

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register at least annually a notice of the existence and character of the system of records,

which notice shall include—

(A) the name and location of the system;
(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; and

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

(f) Agency rules

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall annually compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) Civil remedies

Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the

individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of legal guardians

For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) Criminal penalties

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

(j) General exemptions

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific exemptions

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that

the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(l) (1) Archival records

Each agency record which is accepted by the Administrator of General Services for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Administrator of General Services shall not disclose the record except to the

agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m) Government contractors

When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(n) Mailing lists

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) Report on new systems

Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.

(p) Annual report

The President shall submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicates efforts to administer fully this section.

(q) Effect of other laws

No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.



3 1761 11468783 3